

Memo

To: Dr. Matt Wagenheim, Chair Academic Program Review Council

From: Dr. Barbara L. Ciaramitaro, Chair Academic Review Committee

Date: 6/14/2012

Re: Information Security & Intelligence Academic Program Review Report

Attached please find the Information Security & Intelligence Academic Program Review Report. Also attached please find comments by Dr. Jim Woolen, Department Head. Please let me know if there is any additional information you need in support of this report.



FERRIS STATE UNIVERSITY

COLLEGE OF BUSINESS

June 14, 2012

AFIS DEPARTMENT

(Accountancy, Finance &
Information Systems)

Certificates:

Undergraduate:

- ❖ Homeland Security:
Digital Security &
Forensics
- ❖ Advanced Studies
in Investment
- ❖ Project
Management

Graduate:

- ❖ Advanced Studies
in Business
Intelligence
- ❖ Advanced Studies
in Design &
Innovation
Management
- ❖ Advanced Studies
in Incident
Response
- ❖ Advanced Studies
in Project
Management

Minors:

- ❖ Accountancy
- ❖ Computer Information
Systems
- ❖ Finance

AAS Programs:

- ❖ Accountancy
- ❖ Computer Information
Systems

BS Programs:

- ❖ Accountancy
- ❖ Computer Information
Systems
- ❖ Computer Information
Technology
- ❖ Finance
- ❖ Information Security
& Intelligence

BS Dual Majors

- ❖ Accountancy &
Finance
- ❖ Accountancy &
Computer Information
Systems

MS Programs:

- ❖ Information Security
& Intelligence

Dr. Matt Wagenheim, Chair
Academic Program Review Council
College of Education & Human Services (SRC 102B)
Ferris State University

Re: DRAFT ISI Program Review - DH Comments

First and foremost, I have the utmost respect for the knowledge, skills, and abilities of the faculty who teach in the Information Security & Intelligence (ISI) program. We are fortunate as an institution and a college to have such knowledgeable individuals in this content area. All of the faculty care about student learning, and are student-centered in their approach to teaching.

This program has evolved from the original creation by the faculty and remains extremely viable in a very competitive market. The program has achieved national attention from the Federal government through attainment of the Center of Excellence designation for Information Assurance by the Department of Homeland Security and the National Security Agency. The faculty are engaged in scholarly endeavors and have obtained Federal grants for research projects. Program faculty are very entrepreneurial and creative in curriculum development, recruitment, and promotion of the program to new audiences.

With the rapid growth of the ISI program, I am concerned about having enough resources for support and sustainability. With such high requirements for faculty credentials (e.g., specific certifications, education, and experience), it will be difficult to find a qualified pool of adjuncts. And, with the field exploding with such high demand for qualified people, it will also become more difficult to compete in the area of compensation.

Under Section 1B (Program Goals), item "d" indicates that the program "includes a strong foundation in business core skills and competencies." Since the ISI program only contains 4 of 10 required core courses for the COB, it does not have a strong business foundation. This fact led to the exclusion of the ISI program from the college's ACBSP accreditation. The program does include a fifth course in business skills (MGMT 350), but this course was originally developed as a hybrid accounting/finance experience for a military program.

The ISI program is of great value to the COB, the University, and the State. In order to sustain growth in the program, additional faculty resources will need to be supported by the University.

Respectfully,

Dr. Jim Woolen, CCP
Department Head

119 South Street, BUS 212
Big Rapids, MI 49307-2284
Phone: (231) 591-2434
Fax: (231) 591-3521
E-mail: woolenj@ferris.edu



Information Security & Intelligence

Academic Program Review

FERRIS STATE UNIVERSITY

2012

Barbara L Ciaramitaro, PhD

APR Committee Chair

APR Members

Douglas Blakemore, PhD

Greg Gogolin, PhD

Gerald Emerick, M.A.

Keith Jewett, M.S.

Table of Contents

SECTION 1: PROGRAM OVERVIEW 3

- A. RELATIONSHIP TO FSU MISSION 4
- B. PROGRAM GOALS 5
- C. PROGRAM VISIBILITY AND DISTINCTIVENESS 10
- D. PROGRAM RELEVANCE 10

SECTION 2: COLLECTION OF PERCEPTIONS 13

- A. CURRENT STUDENT SURVEY RESULTS 13
 - SUMMARY OF RESULTS 13
- B. ISI ALUMNI SURVEY RESULTS 20
 - SUMMARY OF RESULTS 20
- C. COB FACULTY SURVEY RESULTS 30
 - SUMMARY OF RESULTS 30
- D. EMPLOYER/ADVISORY BOARD PERCEPTIONS 33
 - SUMMARY OF RESULTS 33

SECTION 3: PROGRAM PROFILE 37

- A. ENROLLMENT 37
- B. QUALITY OF CURRICULUM AND INSTRUCTION 39
- C. COMPOSITION AND QUALITY OF THE FACULTY 40

SECTION 4: FACILITIES AND EQUIPMENT 42

SECTION 5: CONCLUSIONS 44

- CHALLENGES 44
- INCOMPLETE INSTITUTIONAL DATA 45
- ISI SWOT ANALYSIS 45
- BENEFIT TO FERRIS STATE UNIVERSITY 46

APPENDICES 48

- APPENDIX A: SURVEYS 49
 - CURRENT STUDENT SURVEY RESULTS 50
 - ALUMNI SURVEY RESULTS 51
 - COB FACULTY SURVEY RESULTS 52
- APPENDIX B: FACULTY VITA 53
 - FULL TIME FACULTY 54
 - ADJUNCT FACULTY 55
- APPENDIX C: COURSE SYLLABI 56
- APPENDIX D: ISIN CHECKSHEETS 57

APPENDIX E: TRACDAT REPORTS 58
APPENDIX F: ISI PROGRAM SWOT ANALYSIS 59
APPENDIX G: NSA COURSE MAPPING 61

SECTION 1: PROGRAM OVERVIEW

One of the most significant challenges facing our country today is protecting our nation against cyber security threats. As the Director of the FBI recently stated in an interview for CNN Money, "There are two kinds of businesses - those that have been hacked and those that will". The Information Security & Intelligence (ISI) program at Ferris State University addresses this challenge head-on through its courses and hands-on technology tools to prepare students to enter the information security profession with appropriate skills and knowledge.

The Information Security & Intelligence Program first offered courses in 2007. As detailed below, the curriculum of the program was developed with input from the U.S. Department of Homeland Security, the Pentagon, and investigative agencies. The Program grew slowly by design as its goal was to recruit highly motivated students able to master the academic and technical skills the program required. This was accomplished through a GPA requirement of 3.0 for high school students and 2.7 for transfer students as well as individual interviews with each student prospect. The program started offering courses on the Grand Rapids Campus in Spring of 2007 and gradually added additional off campus locations including Traverse City, Big Rapids, and Delta. The program has experienced over 3000% growth as its enrollment increased from 3 students in the Fall of 2007 to 116 students in the Fall of 2011. The program continues to expand its campus locations, courses are being offered at Lansing and Harper Woods (Wayne County) in Fall of 2012. Efforts are also underway to develop an online version of the program for active and veteran military personnel. A detailed look at enrollment is included in Section 3 of this report.

The ISI Program received National attention in June 2011, when it formally received its designation as National Center of Academic Excellence in IA Education (CAE/IAE) by the NSA (National Security Agency) and the DHS (Department of Homeland Security). Ferris successfully mapped its ISI (Information Security & Intelligence) and ISM (Information System Management) programs classes against all six NSA standards

making it one of very few universities in the country to have achieved that level of mapping and the CAE/IAE designation.

A. RELATIONSHIP TO FSU MISSION

We believe the ISI program is in alignment with the FSU mission as shown in the following table.

FSU Mission	Information Security & Intelligence
Successful Careers	Alumni survey results indicate most ISI student alumni felt that the ISI program prepared them for successful careers.
Responsible Citizenship	All core courses include the study of ethics and professional responsibility as part of their course objectives.
Lifelong Learning	Courses encourage ongoing commitment to staying abreast and knowledgeable about current information security threats and countermeasures as an important element of information security professionalism. This is encouraged through recommended involvement with professional organizations such as ISC2, ISACA, and ISSA.
Partnerships	The ISI program is built upon strong partnerships with community colleges including Delta, Northwestern and Grand Rapids Community College. New partnerships with Lansing Community College and Wayne County Community

	College will result in ISI course offerings in fall of 2012. New efforts in motion to partner with military organizations to offer the ISI program in an online environment for military personnel.
Global economy and society	The ISI program and its concentrations emphasize the need to view information security as a global challenge. Specific examples include the emphasis in project management on building and managing cross-cultural project teams and the new National Security Concentration which focuses on global security issues.

B. PROGRAM GOALS

The mission of the Information Security & Intelligence Program is to provide high quality undergraduate graduate instruction in Information Security & Intelligence using the most current technologies and continuous improvement management philosophies in an innovative, stimulating, and globally diverse learning environment.

- a. Introduces students to leading edge cyber security technologies such as digital forensics, visual analysis, mobile forensics, social media forensics, GIS (global information systems), and malware.
- b. Promotes solid intelligence analysis skills.
- c. Integrates global competence, diversity, and ethics into each course offering.
- d. Includes a strong foundation in business core skills and competencies.

1) State the goals of the Program.

The Ferris Information Security & Intelligence (ISI) Program is at the forefront in its response to the need for skilled workers in Information Security/Data Analysis/Digital Investigation and Forensics. The ISI program has several important components in preparing students for successful information security professions.

- **Hands on experience with a variety of best in class Information Security technologies.**
 - Digital Forensics
 - Visual Analysis
 - Penetration Testing
 - Networking and Linux
- **Relevant curriculum with classes focused on emerging trends and threats.**
 - Zero Day Exploits
 - Mobile Device Security and Management
 - Data Loss Prevention
 - Cloud Computing
 - Social Engineering
- **Emphasize core problem solving skills in all classes.**
- **Align Information Security education with key concerns of Information Security Professionals in various domains**
 - Business
 - Law Enforcement
 - Military and Intelligence
- **Encourage student participation in information security organizations and cyber security contests.**
 - Intercollegiate Cyber Defense Competition
 - DC3 Digital Forensic Challenge

- **Encourage student networking with information security organizations such as Infragard, ISACA, ISSA and NAISG.**
- **Collaboration and Partnerships**
 - Strong partnerships with community colleges including Delta, Northwestern and Grand Rapids Community College. New partnerships with Lansing Community College and Wayne County Community College
 - Engaged with security professionals in business, law enforcement, homeland security and military agencies.
 - Offers dual enrolled programs to high school students introducing them to the study of information security.
 - The ISI Advisory Board includes the senior managers and leaders of a variety of businesses and security focused agencies throughout Michigan and serve as a source of review and advice from potential employers of our students.
 - In addition to partnership with external parties in the business, government and law enforcement, the ISI Program also partners internally to develop and support innovative academic program offerings.
 - The undergraduate Project Management Certificate offering was developed in partnership with the ISI, CIS, and Management Departments. As a result of this partnership, 3 new project management courses were developed by ISI faculty as part of the Certificate offering.
 - The undergraduate Medical Informatics Minor was developed in partnership with the College of Allied Health, ISI, and the Marketing Department. As a result of this partnership, the ISI faculty developed a special course in Business Intelligence in Health Care as part of the minor.

2) Explain how and by whom the goals were established.

The ISI Program was developed with input from the U.S. Department of Homeland Security, the Pentagon, and investigative agencies. Its uniqueness includes providing hands on utilization of state of the art technology. Additionally, this program is uniquely positioned to satisfy the education credential necessary for students to be licensed as Professional Investigators in the State of Michigan, while our computer forensics coursework is accepted for meeting the education requirement to site for computer forensic examinations.

In June 2011, Ferris State University formally received its designation as National Center of Academic Excellence in IA Education (CAE/IAE) by the NSA (National Security Agency) and the DHS (Department of Homeland Security). Ferris successfully mapped its ISI (Information Security & Intelligence) and ISM (Information System Management) programs classes against all six NSA standards making it one of very few universities in the country to have achieved that level of mapping and the CAE/IAE designation. A complete mapping of our ISI courses to the stringent requirements of the NSA CNSS standards is included in full as Attachment G.

3) How do the goals apply to preparing students for careers and meeting employer needs in the community/region/marketplace?

Protecting the security of our country and businesses is one of the most pressing needs facing our society. As a result, information security professionals are in high demands in both government and private industry. Recent studies indicate that systems analysts, who include security analysts, can look forward to estimated job growth of 53 percent through 2018, making this the second fastest-growing occupation in the nation. Homeland security jobs are expected to remain in high demand as national security is among the highest priorities of our government. One area that should see substantial and ongoing growth is jobs

related to cybersecurity. Additionally, the federal government's new Cyber Security Command in Fort Meade, Maryland, has created an IT hiring hot spot in 2011, but companies of all sizes and in every location will need security professionals with the skills to keep their data protected, he says.

We validate the ISI programs ability to successfully prepare information security professionals in 3 ways:

- Our designation as a Center of Academic Excellence in Information Assurance Education demonstrates that we have been vetted at the highest levels of security expertise including the National Security Agency, Department of Homeland Security, and the Department of Defense. As a result of this designation, our students receive preferential treatment when applying for positions in the government or government contractors. Additionally, this designation is highly regarded in private industry and allows our students to be regarded highly when considered for information security positions.
- As will be detailed in a later section of this Review, our alumni have indicated in their Survey results that the ISI program contributed to their professional success.
- An important part of our validation is our communication with our ISI Advisory Board who also serves as employers for many of our students. On an annual basis we meet with our Advisory Board to verify that our Program remains relevant and distinctive. Our Advisory Board has continuously approved of our Program's direction adding their ideas for areas of further development such as the project management concentration which is now in place.

4) Have the goals changed since the last program review?

This is the first program review for the Information Security & Intelligence program which began in 2007.

C. PROGRAM VISIBILITY AND DISTINCTIVENESS

The ISI Program was developed with input from the U.S. Department of Homeland Security, the Pentagon, and investigative agencies. Its uniqueness includes providing hands on utilization of state of the art technology.

In June 2011, Ferris State University formally received its designation as National Center of Academic Excellence in IA Education (CAE/IAE) by the NSA (National Security Agency) and the DHS (Department of Homeland Security). Ferris successfully mapped its ISI (Information Security & Intelligence) and ISM (Information System Management) programs classes against all six NSA standards making it one of very few universities in the country to have achieved that level of mapping and the CAE/IAE designation.

D. PROGRAM RELEVANCE

Predictions of high growth in the information security sector come from various sources:

“The volume, seriousness and sophistication of security threats aimed at public and private organizations will continue to expand in 2011, making security a hot sector for IT employment. The federal government’s new Cyber Security Command in Fort Meade, Maryland, created an IT hiring hot spot in 2011, but companies of all sizes and in every location will need security professionals with the skills to keep their data protected.”

Source: 2011 IT Outlook retrieved from <http://career-advice.monster.com/job-search/company-industry-research/2011-it-hiring-outlook/article.aspx>

“Security is among the fastest-growing fields in the IT sector. The Bureau of Labor Statistics' Career Guide to Industries identifies computer services as “among the five industries with the largest job growth,” with a 45 percent increase in jobs between 2008 and 2018. A major factor in this growth, explains the BLS, is “the increasing need to maintain network and computer system security.” Systems analysts, who include security analysts, can look forward to estimated job growth of 53 percent through 2018, making this the second fastest-growing occupation in the nation. Systems security is among the highest-demand security specialty, along with security software development, disaster recovery services and custom security programming.”

Source: Computer System Computer Security Analyst Salary and Outlook retrieved from <http://www.schools.com/news/computer-systems-security-analyst-salary-career-outlook.html>

“Employment of information security analysts, web developers, and computer network architects is projected to grow 22 percent from 2010 to 2020, faster than the average for all occupations. Job prospects for all three occupations should be favorable.”

Source: Occupational Outlook Handbook retrieved from <http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts-web-developers-and-computer-network-architects.htm>

“Another expected set of skills in demand is around information security, with 1,680 available jobs listed on Dice now – a 109% increase.”

Source: IT Job Outlook 2011 retrieved from <http://www.serviceassurancedaily.com/2011/01/it-job-outlook-2011-high-tech-skills-in-demand/>

Current Career Opportunities for Information Security Students: Opportunities exist in Business, Law Enforcement and Government

- Information Security Crime Investigator
- Security Architect
- Security Auditor
- Penetration Tester (Ethical Hacking)
- Malware and Intrusion Analyst
- Secure Code Developer
- Disaster recovery/business continuity
- Vulnerability Researcher
- Network Security Engineer
- Chief Security Officer
- Legal prosecution and defense of computer crimes

Sample Average Salaries of Information Security Professionals

- Booz Allen – Information Security Associate - \$107,989
- Wells Fargo – Information Security Engineer - \$93,835
- Verizon – Senior Network and Information Security Engineer - \$100,383
- Bank of America – Information Security Engineer - \$79, 533
- Intuit – Information Security Analyst - \$121, 600
- Deloitte – Information Security Analyst - \$90, 333
- Wipro – Associate Consultant Information Security - \$56,305

Source http://www.glassdoor.com/Salaries/information-security-salary-SRCH_KO0,20.htm

SECTION 2: COLLECTION OF PERCEPTIONS

A. CURRENT STUDENT SURVEY RESULTS

26% response rate (31 responses out of 120 surveys sent)

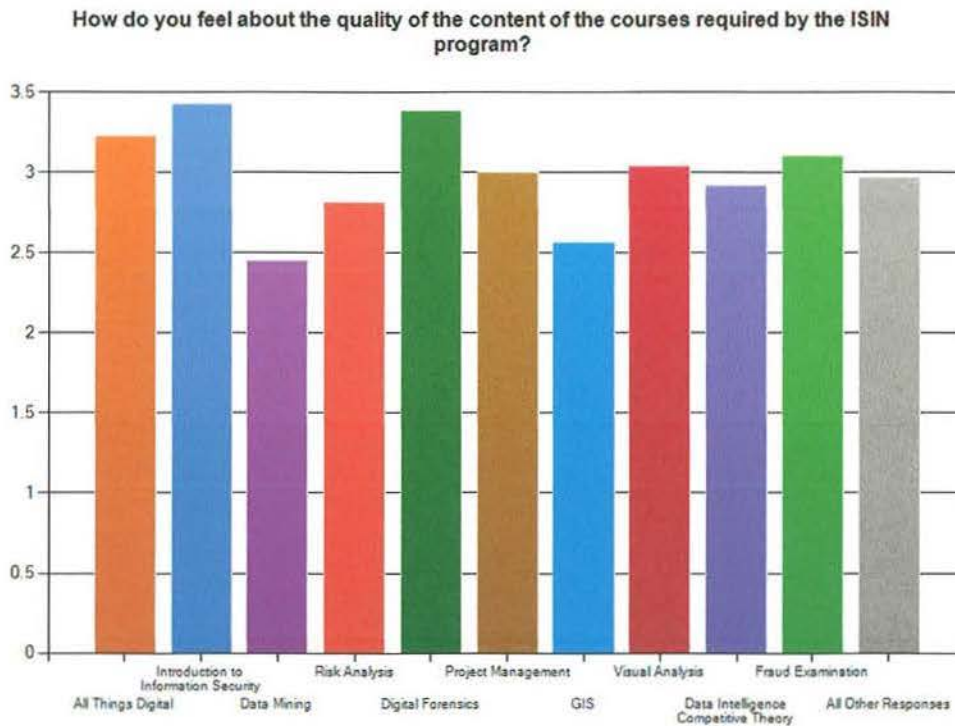
Summary of Results

- All courses taught by ISI department faculty (ISIN, HSCJ and PROJ courses) received ratings in quality of content and instruction received scores between 3 and 4 on a 4 point rating scale.
- Courses taught by other departments as part of the ISI program received scores between 2.5 and 3 on of 4 point rating scale
- The existing digital forensics concentration and the new national security and secure software development concentrations were considered the most relevant of concentrations offered through the program. Foreign language and GIS/Data Mining were considered by students to be the least relevant.
- Half of the students felt that the ISI courses had adequately preparing them for future jobs in information security fields (54.5% Agreed). This certainly leaves room for significant improvement and challenges the program to ensure that its courses and concentrations are consistent with, and relevant to current and future job opportunities.
- 80% of the students stated that if given the opportunity they would choose the Ferris State ISI program again. Students also generally considered the courses to be intellectually challenging (54% Agreed and 36% Strongly Agreed).
- 72% of the students felt that the academic advising they received from ISI faculty was accurate and helpful.
- 45% of the alumni has pre-employment before they entered the program; 27% found employment within 6 months; 18% continued their education; and 9% stated that they never found employment. The 9% who have not found employment is indicative of one area of concern about which the Program must be clear in the expectations it establishes for students and their job opportunities. Depending on the location of the campus, there are some areas of Michigan

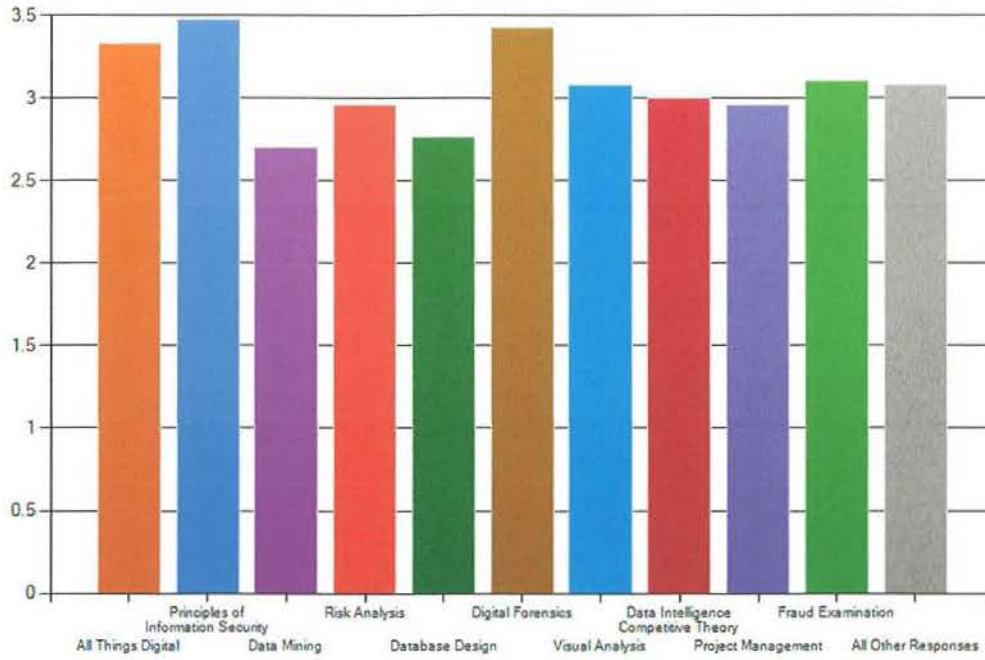
such as Traverse City, where job opportunities in information security are few and far between. It is important to be very clear with students at the outset of the Program, that geographic limitations in their job search will limit their opportunities to find work in this field.

- In terms of current salaries, 40% of alumni are earning between \$35,000 and \$40,000 annually; 40% are earning between \$50,000 and \$70,000 annually ; and 20% are earning \$70,000 or more annually.
- 72% of the alumni felt a strong sense of camaraderie among the ISI students and faculty members and 100% of the alumni felt that the ISI faculty members cared about their progress.

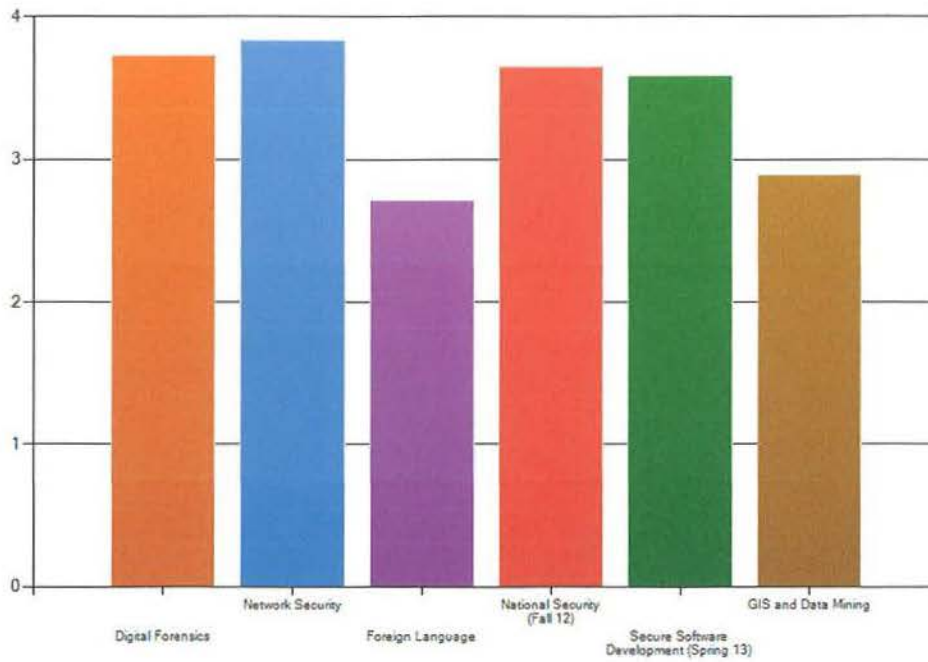
Detailed survey results follow in summary graphs and are included in detail in Attachment A.



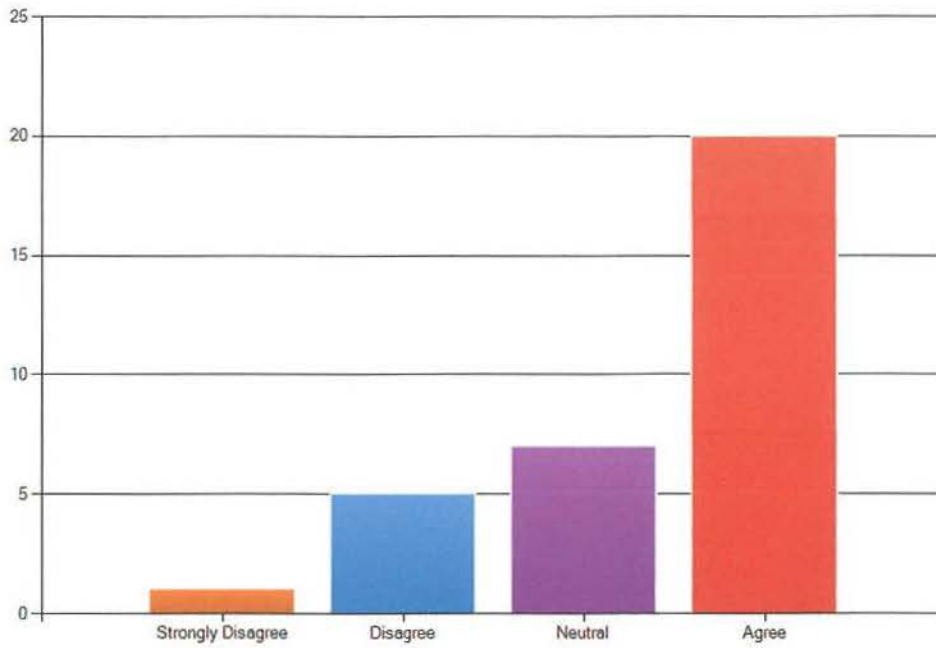
How do you feel about the faculty instruction and delivery of the courses in the ISIN program?



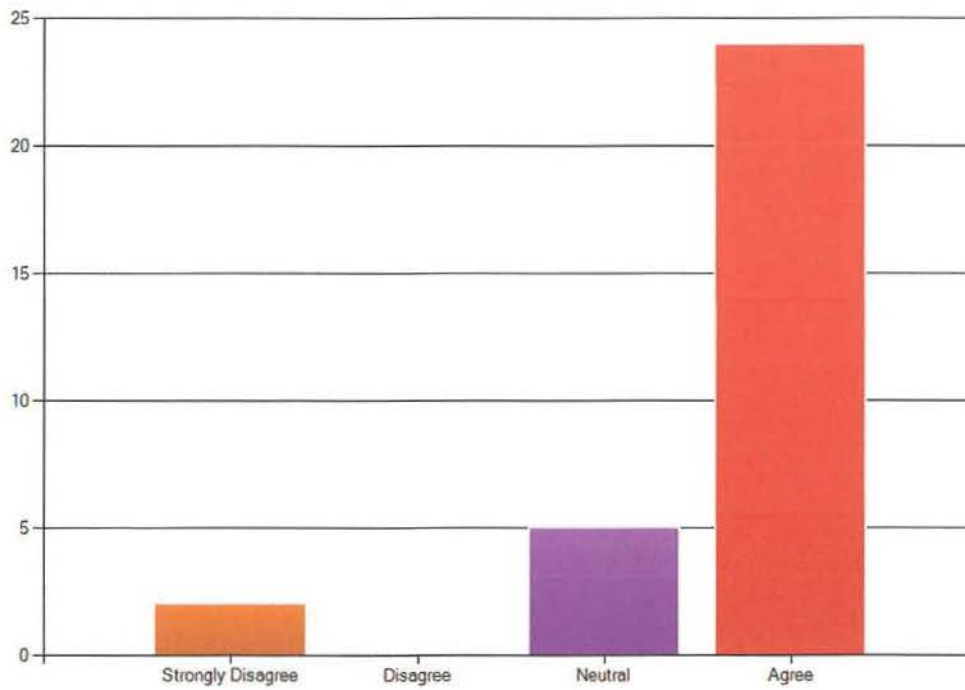
How do you feel about the relevance of the concentrations offered in the ISIN program?



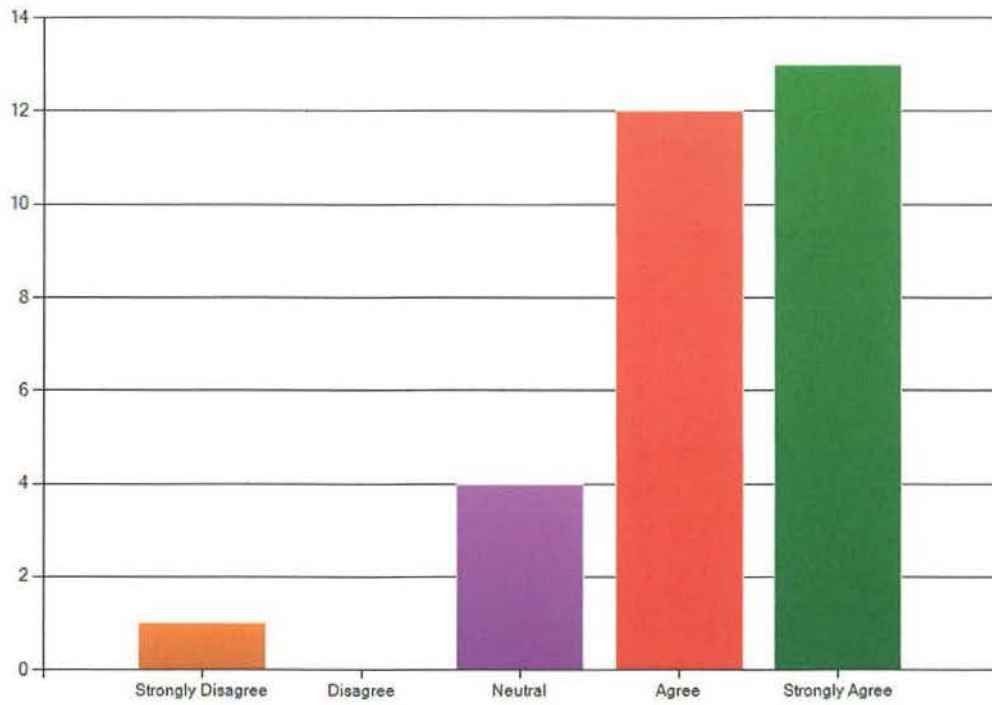
The ISIN program provides me with enough background in Information Security and Intelligence to confidently seek employment in a related field.



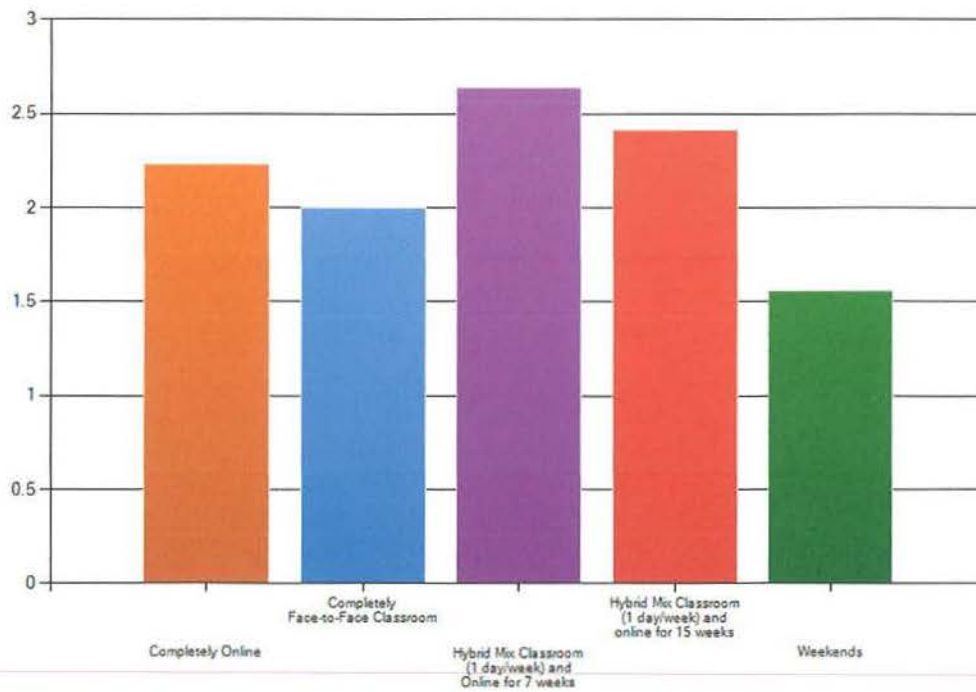
The academic advising that I receive from ISIN faculty is accurate and helpful.



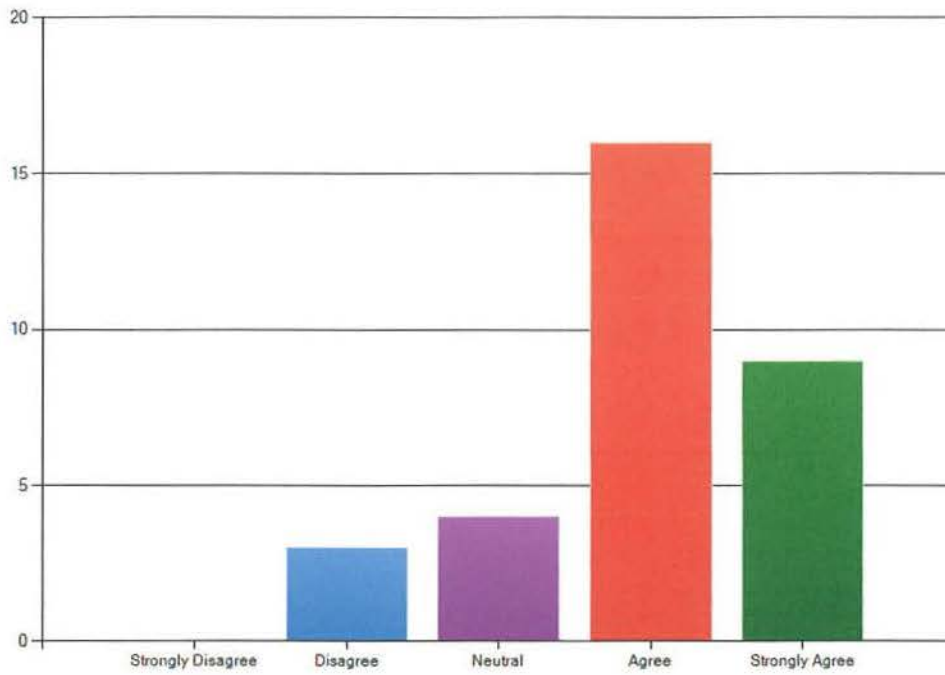
I am generally well satisfied with the ISI curriculum.



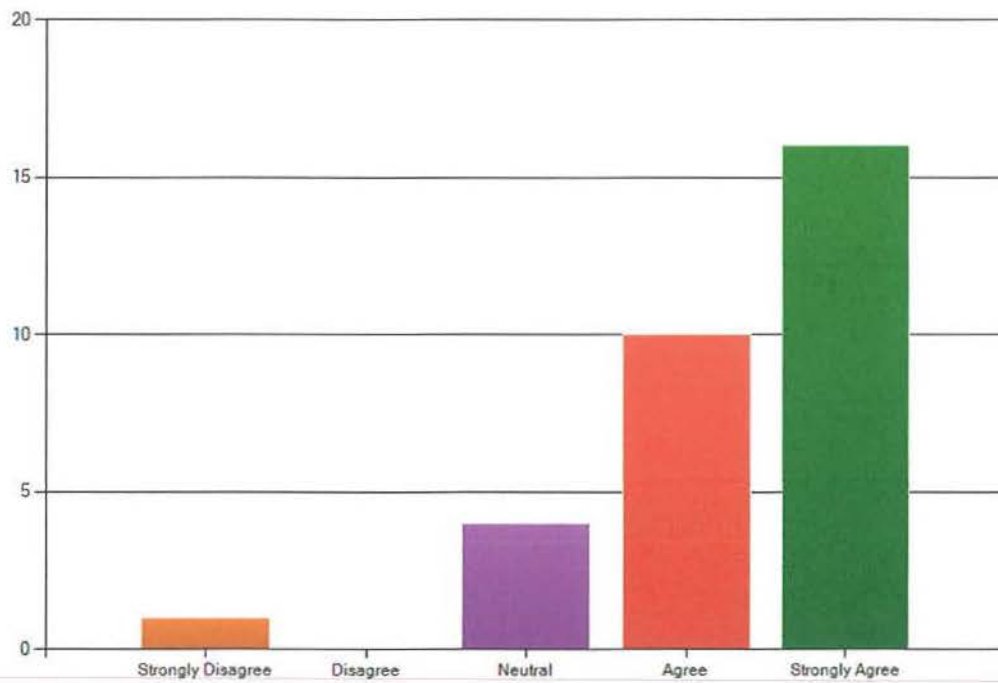
Please indicate your preferred approaches to course offerings?



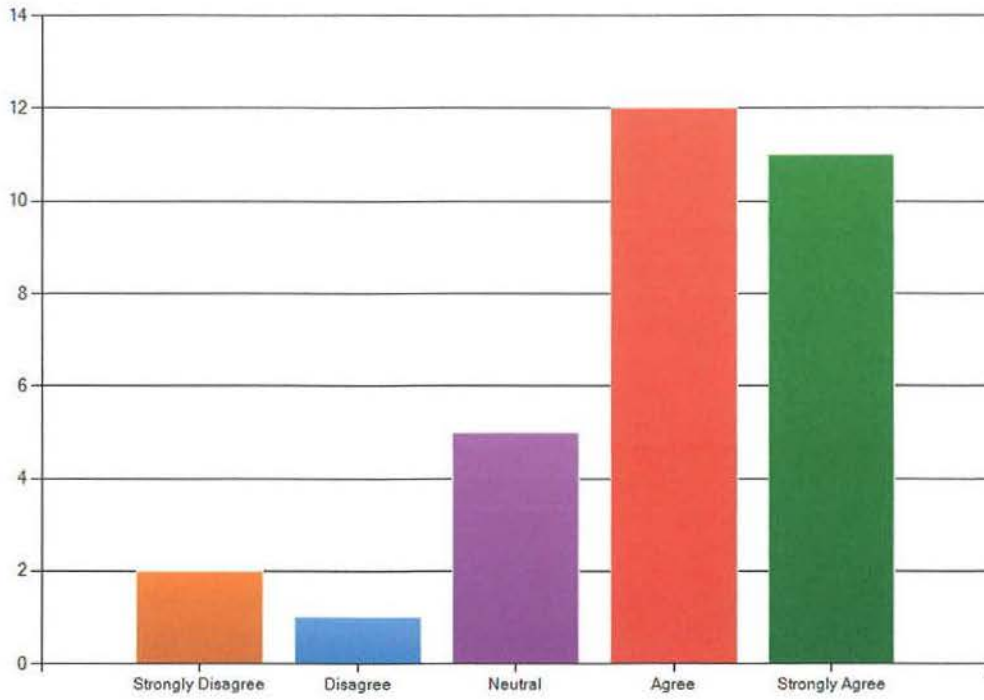
I feel that in general the ISIN courses are intellectually challenging.



There is a feeling of camaraderie (friendliness) in the ISIN program among students and faculty.



I feel that the technology resources used in the ISIN program are adequate and reliable.



B. ISI ALUMNI SURVEY RESULTS

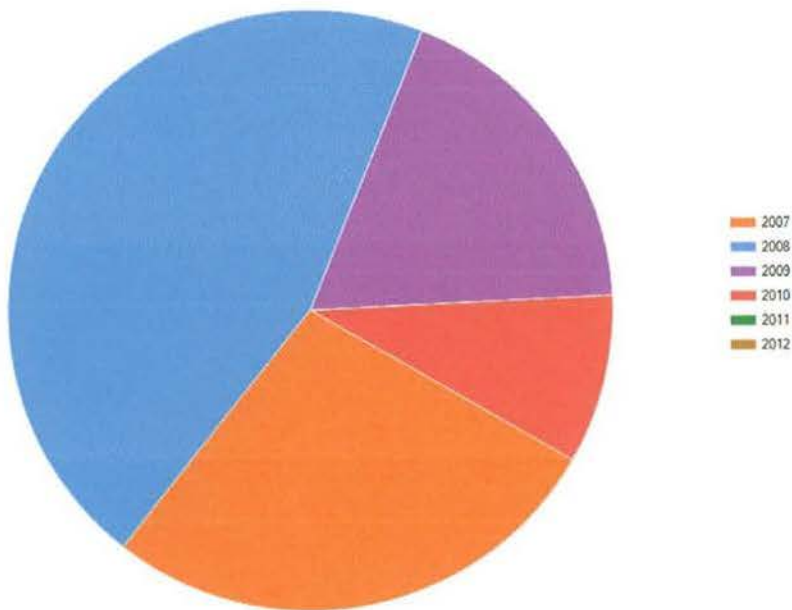
55.5% response rate (10 responses out of 18 surveys sent)

Summary of Results

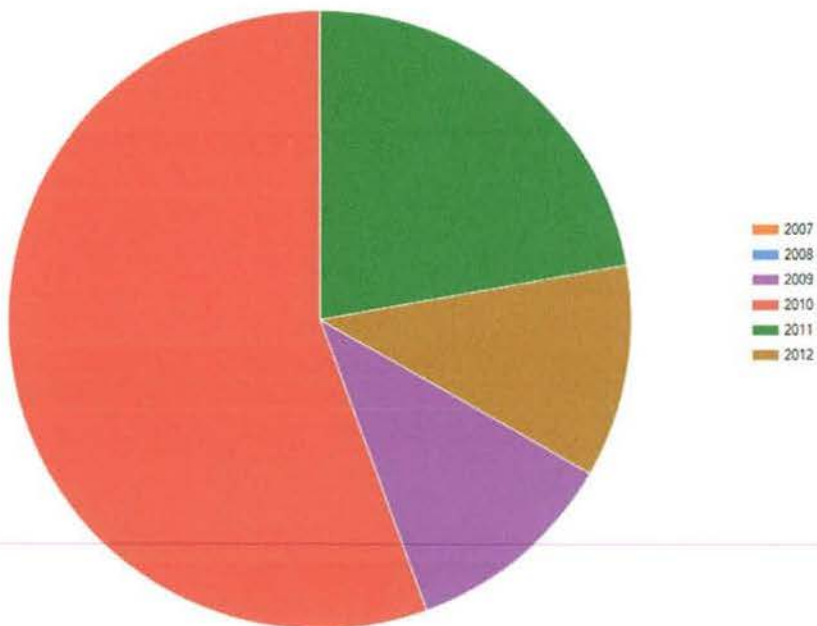
- The alumni results mirror the current student responses in that all courses taught by ISI department faculty (ISIN, HSCJ and PROJ courses) received ratings in quality of content and instruction received scores between 3 and 4 on a 4 point rating scale.
- Courses taught by other departments as part of the ISI program received scores between 2.5 and 3 on of 4 point rating scale
- Similar to the current student results, the existing digital forensics concentration and the new national security and secure software development concentrations along with network security were considered the most relevant of concentrations offered through the program. Foreign language and GIS/Data Mining were considered by students to be the least relevant.
- The far majority of the students were confident that the ISI courses were adequately preparing them for future jobs in information security fields (64.5% Agreed).
- Students were positive in their perception of the overall ISI program (40% Agreed and 43% strongly agreed. Students also generally considered the courses to be intellectually challenging (61% Agreed and 29% Strongly Agreed).
- 77% of the students felt that the academic advising they received from ISI faculty was accurate and helpful.
- 75% of the students preferred or purely online classes as well as the 7 week course format.
- 51% of the students felt a strong sense of camaraderie about the ISI students and faculty.
- 73% of the students felt that the technology resources utilized in the ISI program is adequate and reliable.

Detailed survey results follow in summary graphs and are included in detail in Attachment A.

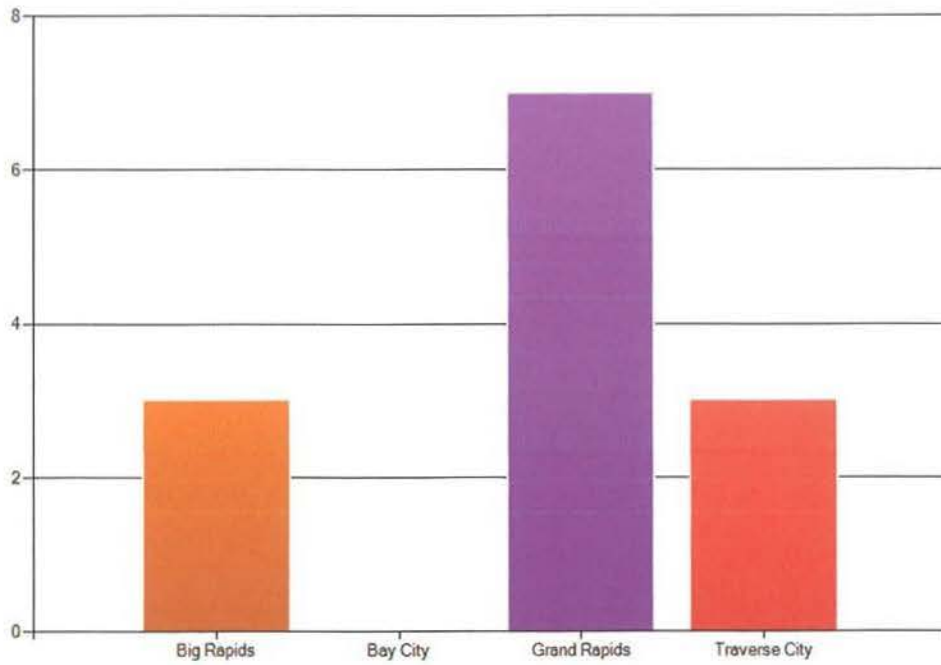
In what year did you enter the ISIN program?



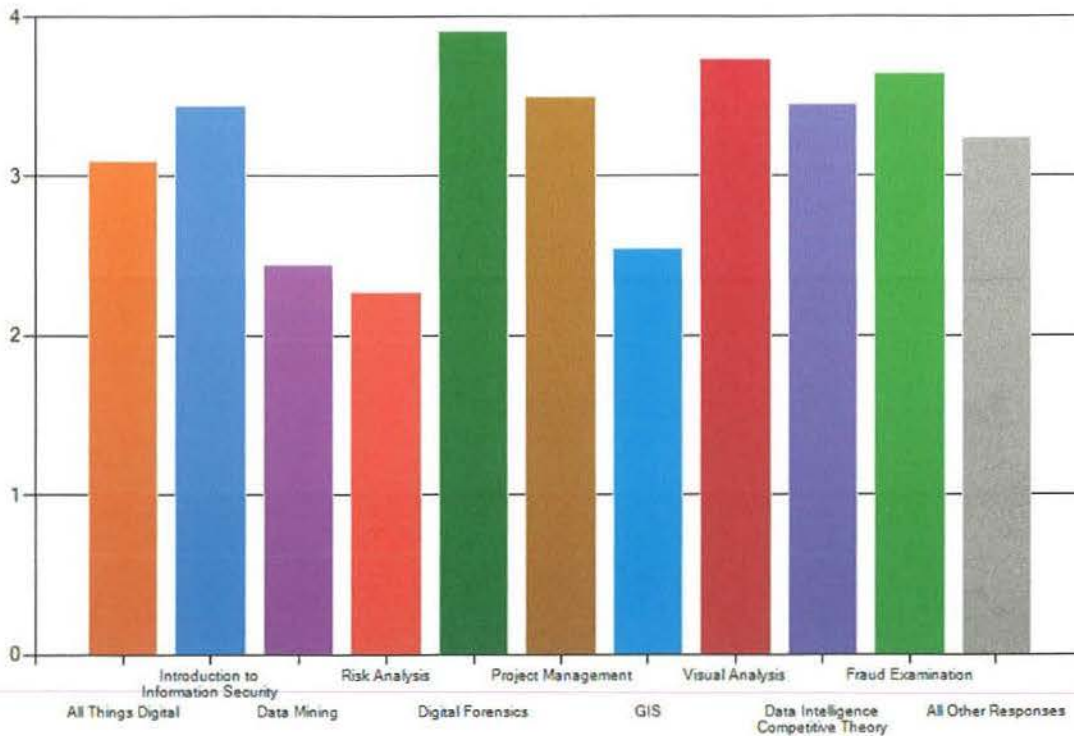
In what year did you graduate or leave the ISIN program?



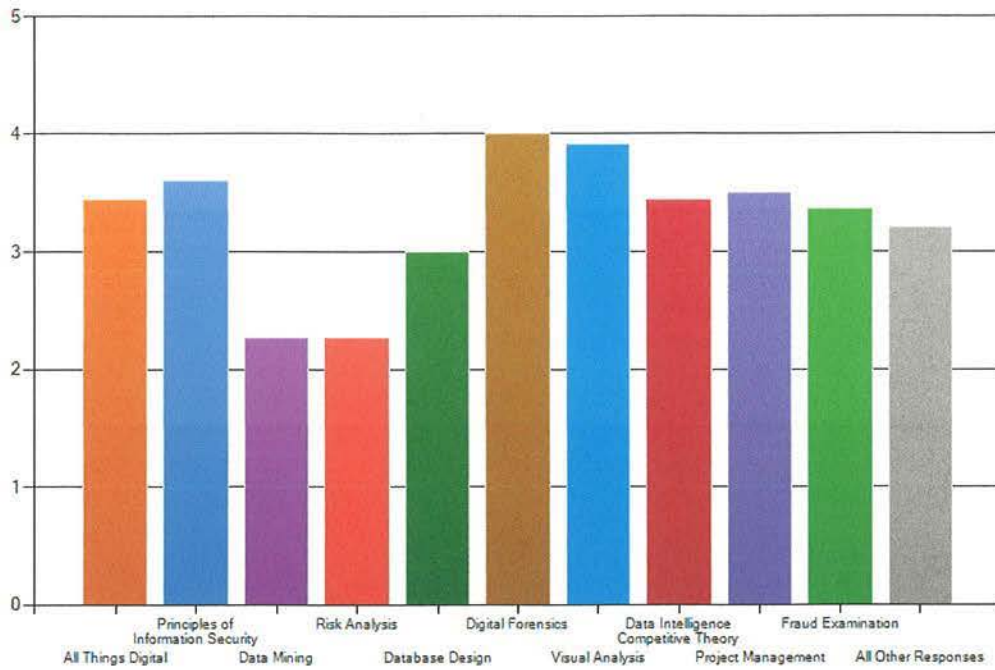
What was the campus location at which you took your ISIN classes?



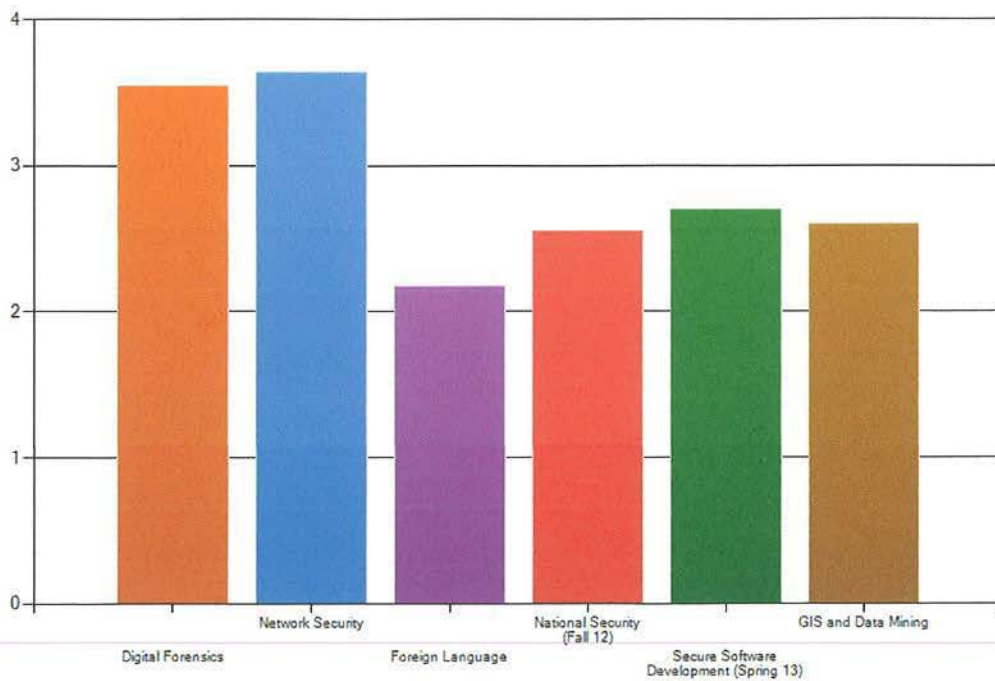
While a student in the ISIN program, how did you feel about the quality of the content of the courses required by the ISIN program?



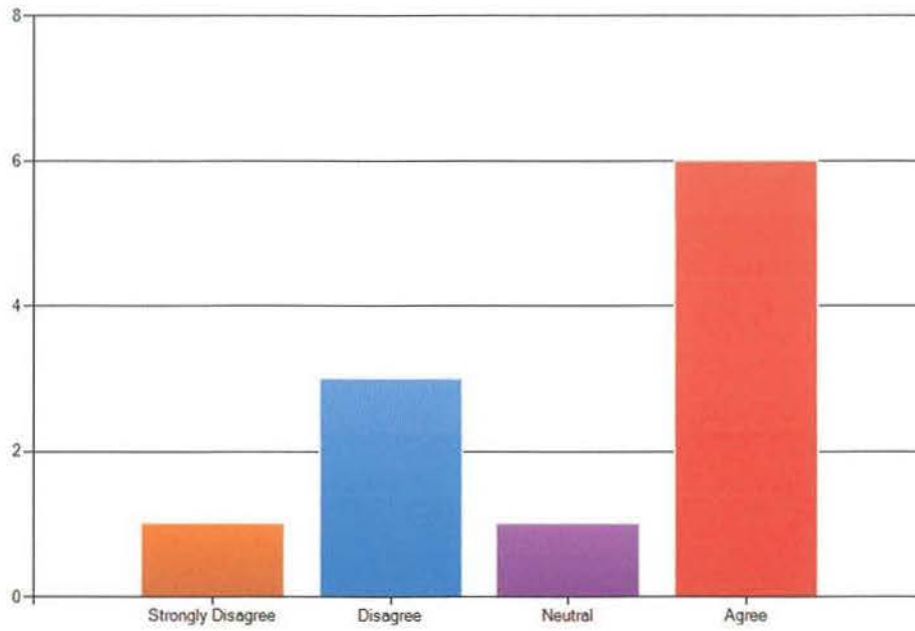
While a student in the ISIN program, how did you feel about the faculty instruction and delivery of the courses in the ISIN program?



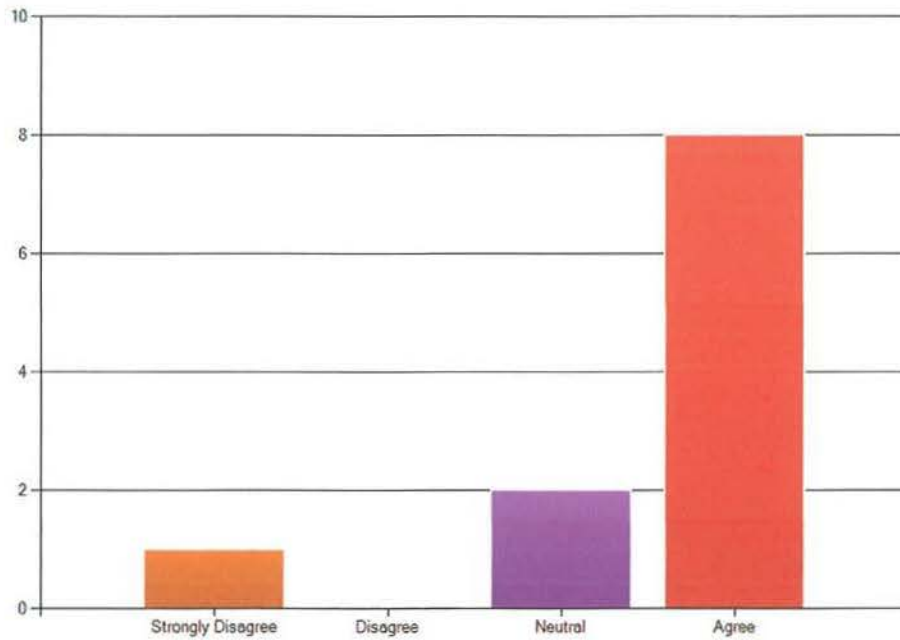
As an alumni of the ISIN program, how relevant are the concentrations offered in the ISIN program?



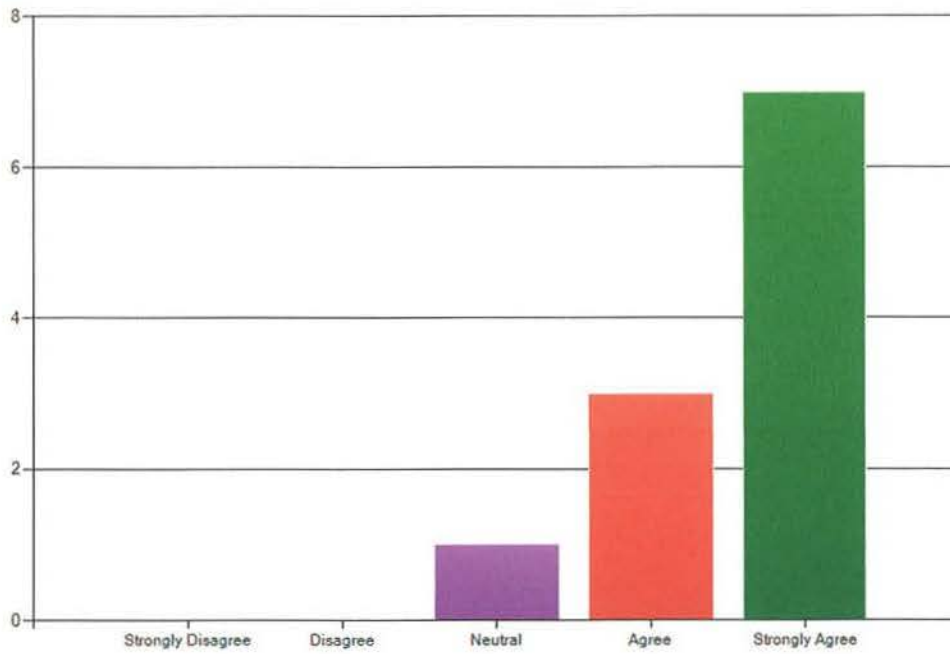
The ISIN program provided you with enough education and skills in Information Security and Intelligence to achieve employment in the ISIN field of your choice



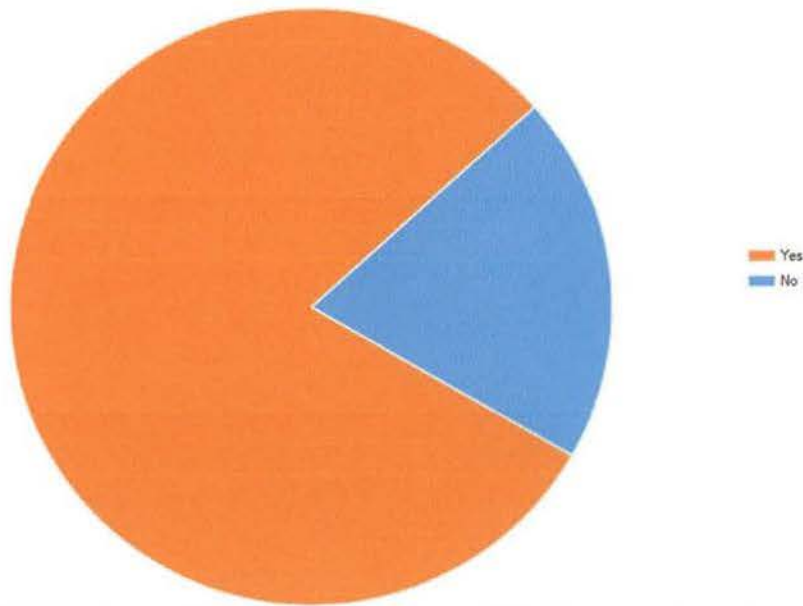
The academic advising that I received from ISIN faculty was accurate and helpful.



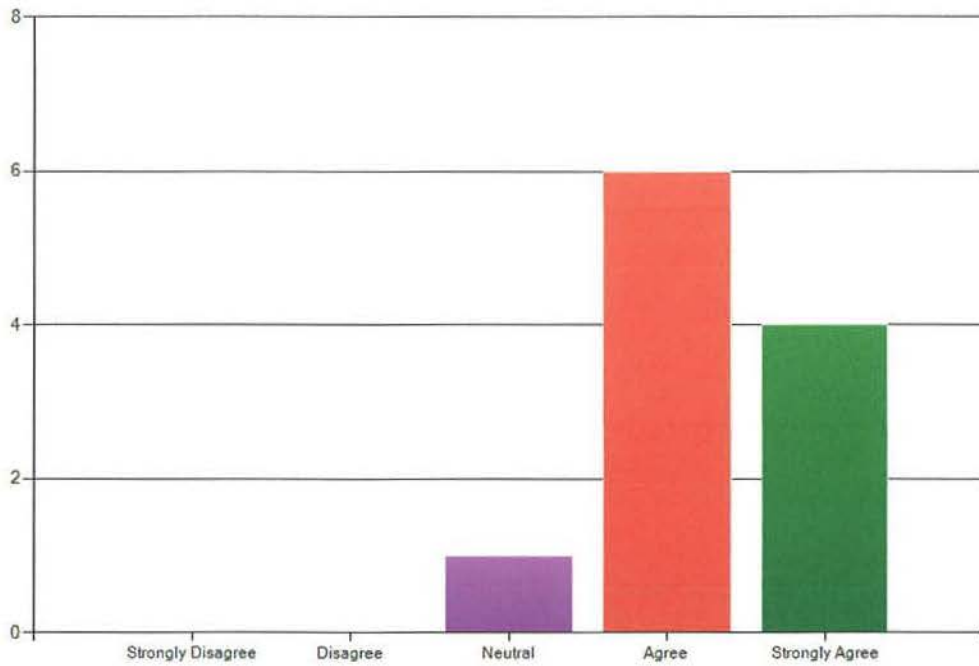
The ISIN program contributed in a positive manner to my ability to problem solve, work on a team, and communicate verbally and in a written format.



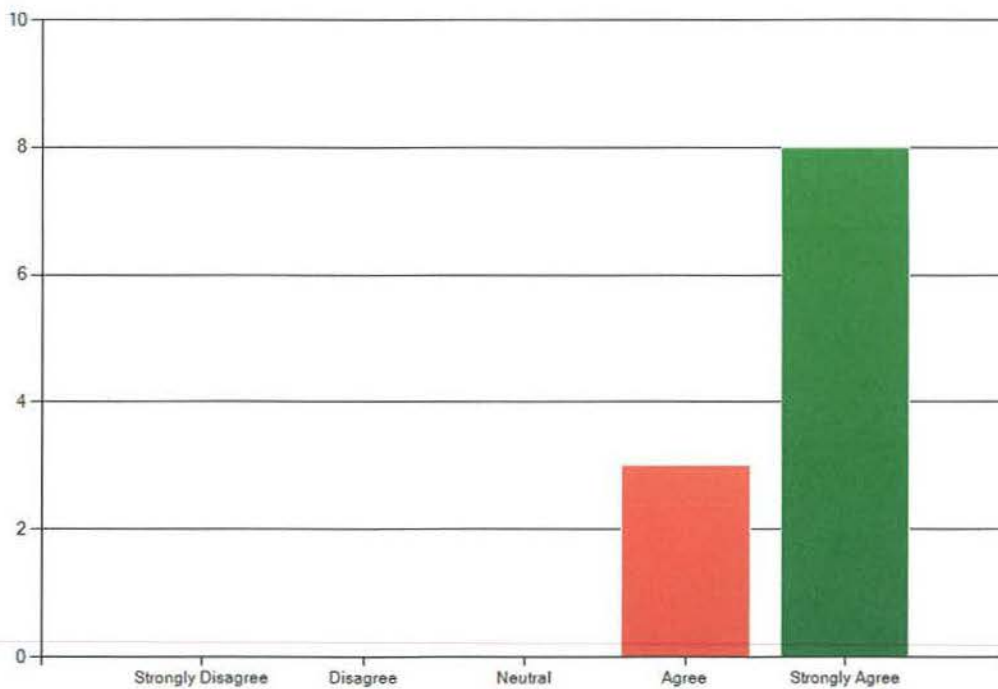
If you could go back and start over, would you choose the Ferris State ISI Program again?



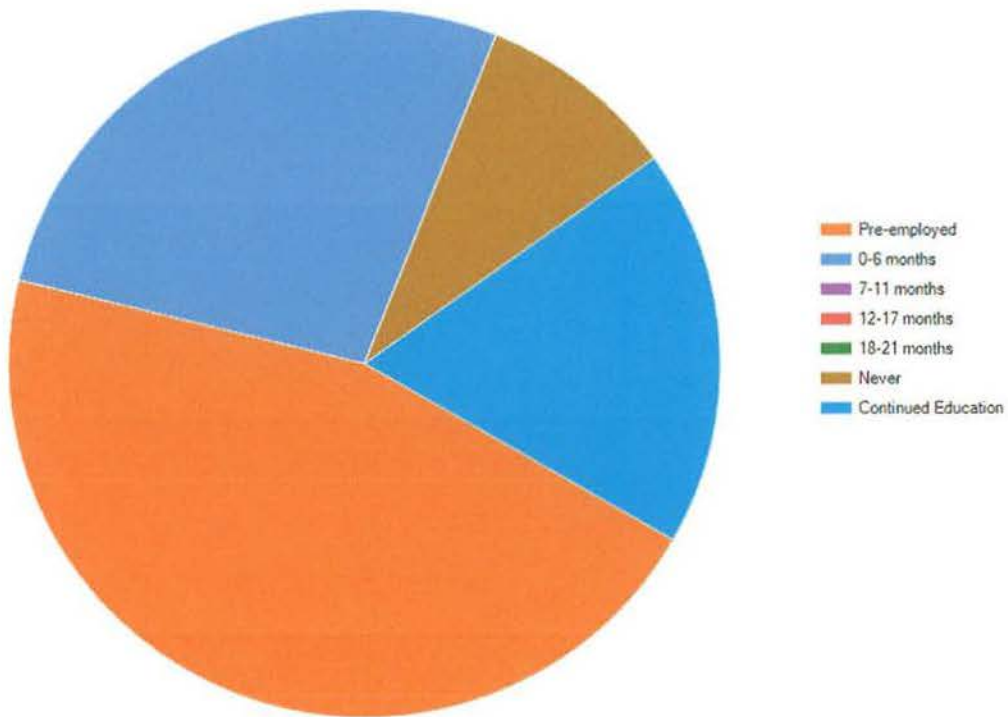
While a student in the ISIN program, I felt that in general the ISIN courses are intellectually challenging.



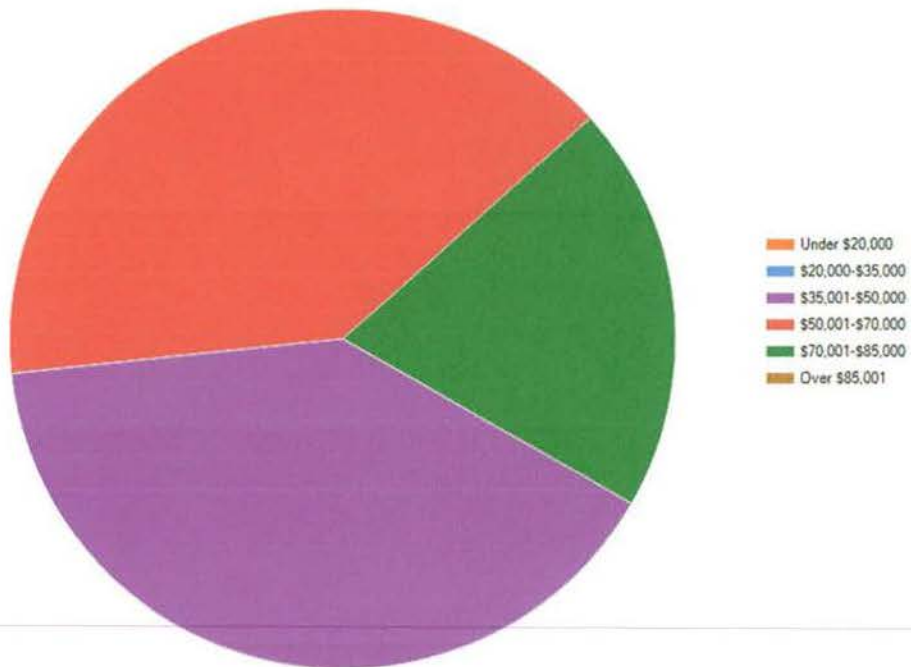
While a student in the ISIN program, there is a feeling of camaraderie (friendliness) in the ISIN program among students and faculty.



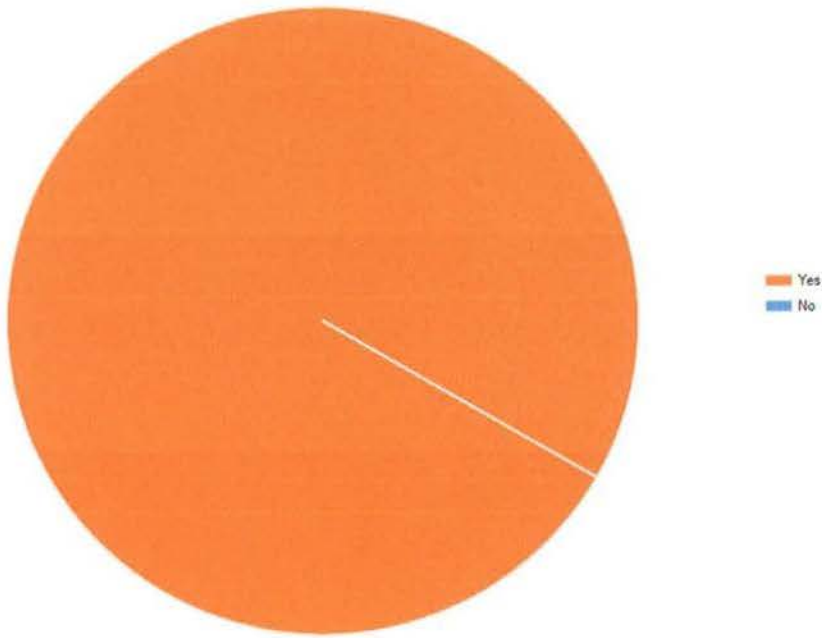
How long after leaving the ISI Program did it take to find employment?



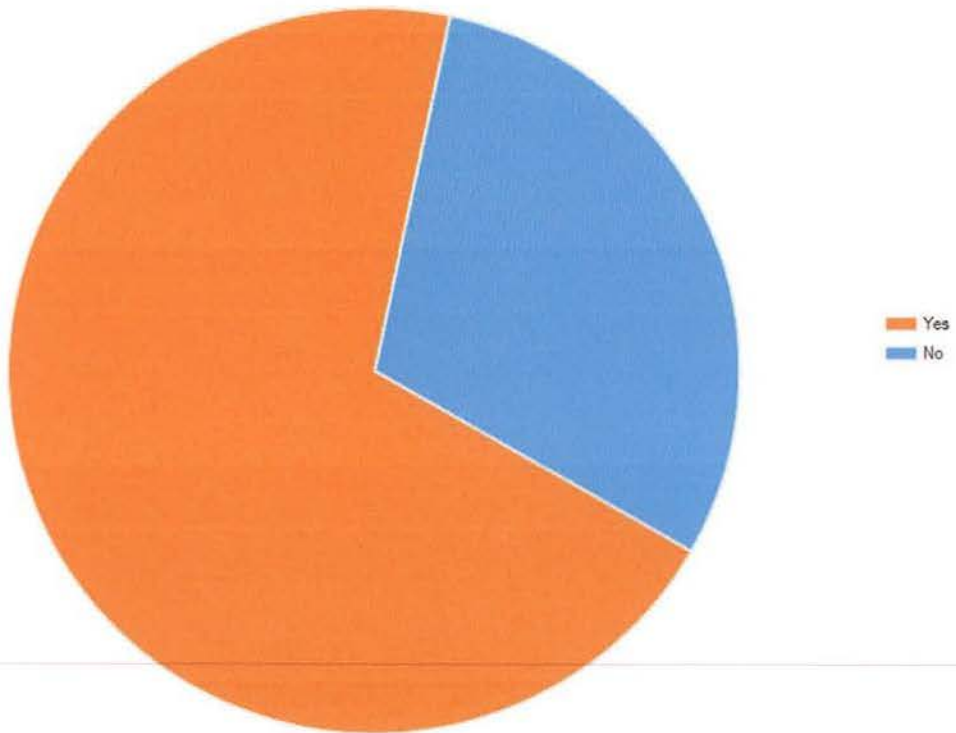
What is your current income range? (U.S. dollars)



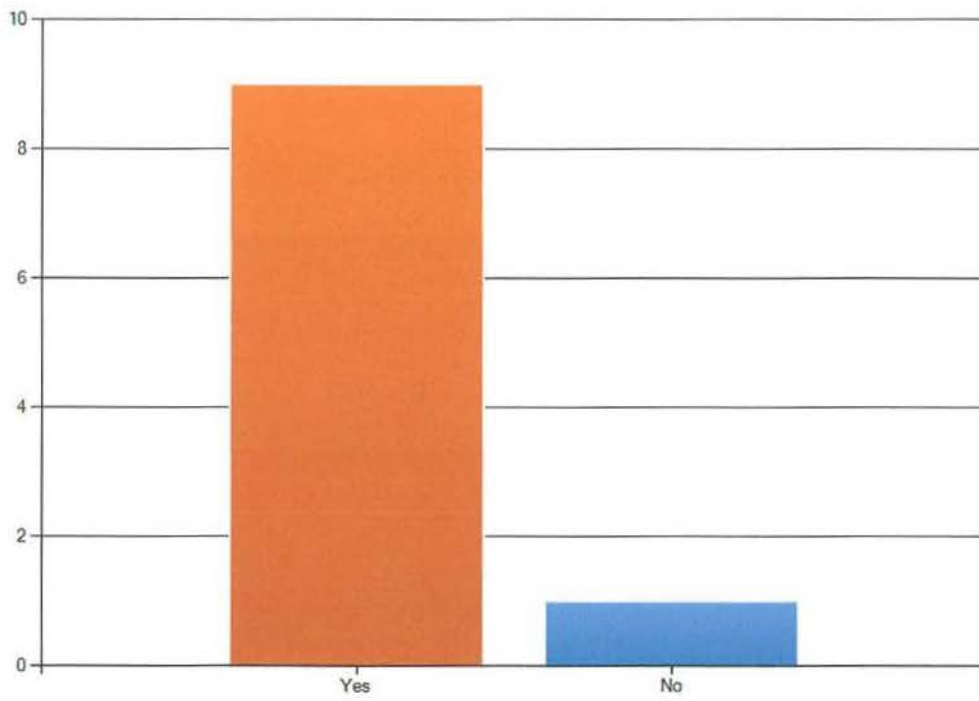
The faculty in the ISIN program cared about my progress.



I am employed in my major or a closely related field.



Would you recommend the ISIN program to others?



C. COB FACULTY SURVEY RESULTS

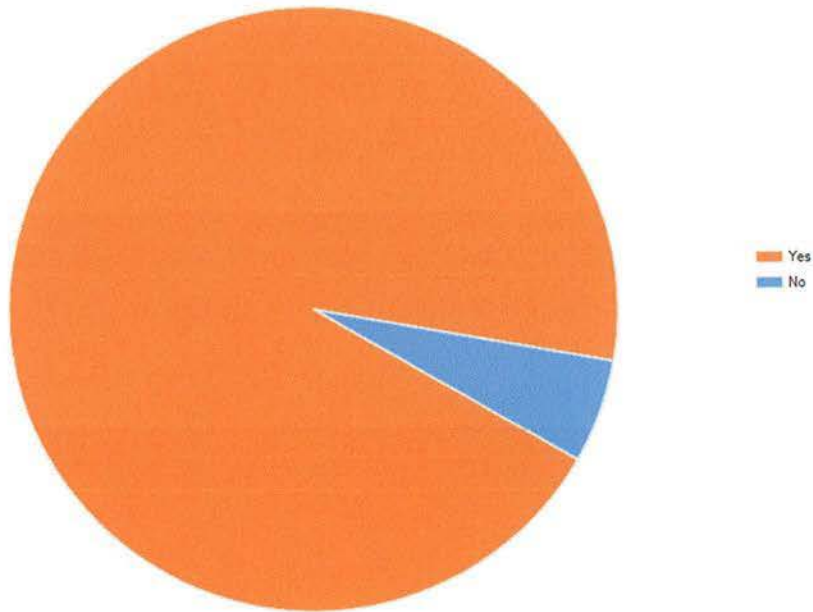
46% response rate (31 responses out of 68 surveys sent)

Summary of Results

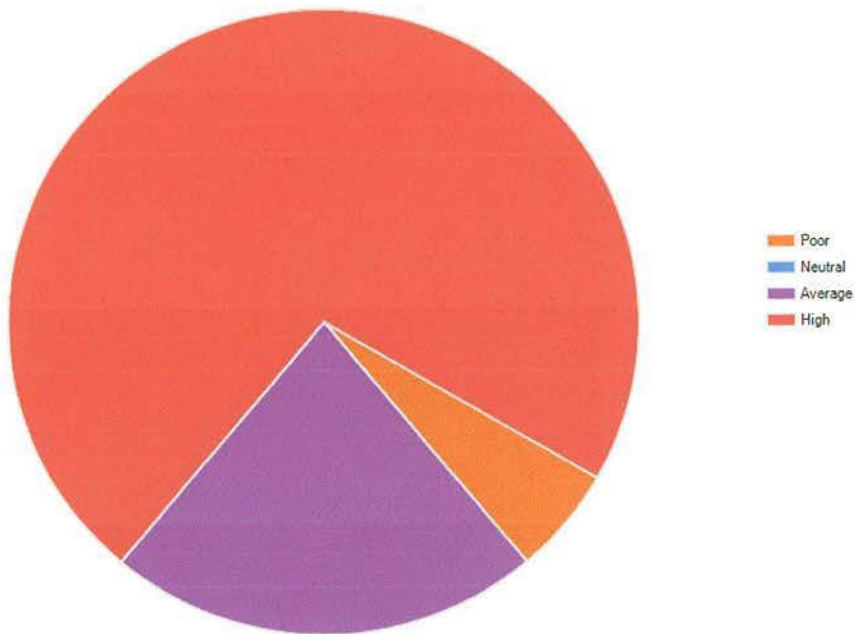
- 94% of COB faculty members are aware of the ISI Program.
- 72% of COB faculty members consider the ISI course content to be of high quality and 61% consider the quality of instruction to be high. This finding causes some concern in the perception of quality of the ISI program from other faculty members in the College of Business. Additional follow-up is recommended to determine areas where ISI faculty could improve the perception of its program to other faculty.
- 89% of COB faculty members consider the ISI program to be relevant for professional careers.

Detailed survey results follow in summary graphs and are included in detail in Attachment A.

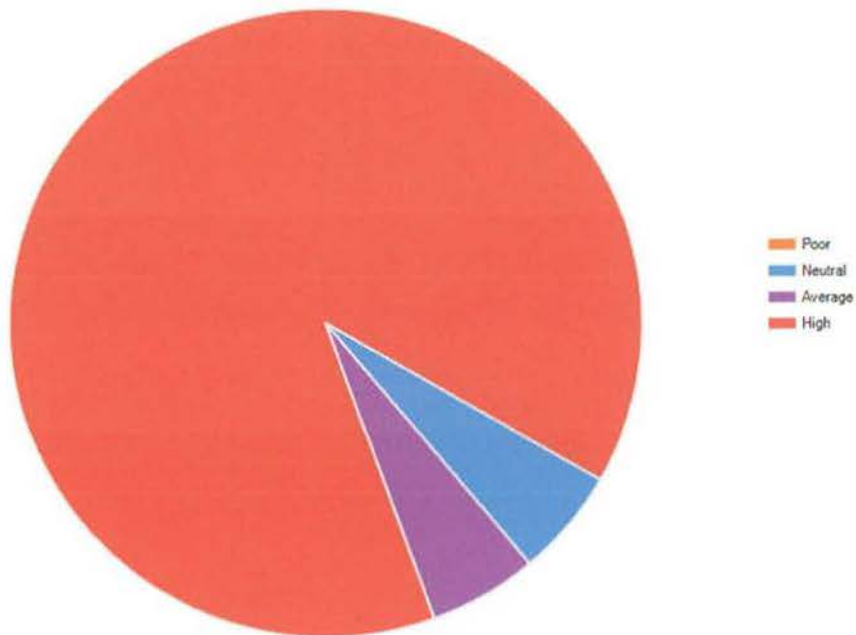
Are you aware of the Information Security & Intelligence program in the College of Business?



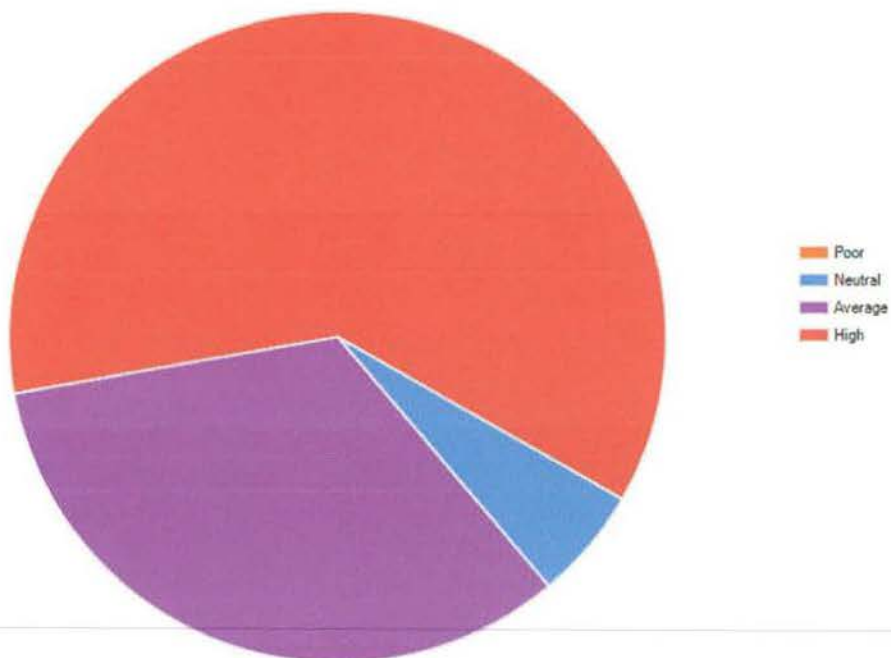
What is your perception of the quality of course content presented in the Information Security & Intelligence Program?



What is your perception of the relevance of the Information Security & Intelligence program to students looking for professional careers?



What is your perception of the quality of instruction in the Information Security & Intelligence program?



D. Employer/Advisory Board Perceptions

Summary of Results

- Due to the newness of the ISI Program and the lack of a solid sample of ISI alumni in IS related professions (out of the 11 survey responses, 46% were pre-employed and 18% pursued continued education), the ISI program relies heavily on its Advisory Board for prospective employer perspectives.
- The ISI/ISM Advisory Board includes leaders and members of various organizations throughout Michigan representing health care, law enforcement, various commercial businesses, and education institutions.
 - Jeff Bleich, Priority Health
 - Sharon Blumeno, Automation alley
 - Ralph Bolen, Motor City Casino
 - Roy Geleman, Hantz Group
 - Steve Hawn, Frontier Corpotation
 - Faith Heidkkila, InfraGard
 - Ted Hutchins, TransAir
 - Therese Iglesias, JDM systems
 - Tom Kish, Michigan State Police
 - Kevin Lasser, Michigan Homeland Security Consortium
 - Stuart McCubbrey, General Motors
 - Mike McIntosh, Amway Global
 - Noah Meister, Boyne USA
 - Michal Moll, Department of Homeland Security
 - David Nehra, Motor City Casino
 - Chris Payne, Priority Health
 - Andrew Patterson, Border Patrol, Department of Homeland Security
 - Matt Roush, Editor, Great Lakes IT Report
 - Ethan Steiger, R.L. Polk
 - Linda Stephens, Kellogg's
 - Jeffrey Vangordon, Department of Homeland Security

- Gene Sauter, Frontier Corp

Meetings of the ISI Advisory Board are held annually in September of each year.

2010 Advisory Board Meeting Notes

In 2010 the Advisory Board focused a great deal of attention on the types of skills and understandings that the ISI/ISM advisory board members expected from students graduating from our program. The following items were mentioned as knowledge areas important for our students. The majority of the discussion focused on the general skills needed by our students rather than specific technical skills as can be seen in the following minutes.

Business Intelligence and Data

There was a lively discussion on the value of understanding how data feeds decision-making. Students are expected to know how to perform data analysis and understand the relevance of their finds to business. In particular, an understanding of data in financial systems was mentioned. Students were expected to understand how databases and data warehouses are designed and implemented such as the translation of business use cases to the star schema. Students should also be familiar with collecting and analyzing data used as metrics such as Google Analytics and other web services data. There was also agreement on the need for students to be comfortable in the role of the business analyst who is able to translate business requirements into data requirements.

Professional Skills

There was unanimous agreement by all advisory board members that many students are unprepared in professional or soft skills such as communication and interpersonal relationships. Several members stated that they would rather choose someone with less technical skills but strong professional skills over a more talented technical applicant. Students need to be able to communicate in a written format with correct business grammar and word usage. They also need to be comfortable with presenting

and critical analysis and discussion. Lastly, they emphasized that students need to learn to listen. More specific concerns emerged from the discussions such as the poor quality of writing they are seeing in their new applicants. Additionally, although they appreciate the growth of social networking, they expect students to be just as comfortable communicating in face to face situations.

Social Media

The advisory board expressed concern over managing the expectations of new employees who want open access to all social media tools at their work. They feel it is necessary to education students on the appropriate use of Social media and how to integrate it with other more traditional forms of business communication.

Security Concerns

Two specific security areas identified as major concerns by the advisory board member including their challenges in balancing privacy, security and usability. They also discussed the challenge of protecting their data from leaving their organization and the need for more education on data loss prevention. Lastly there was discussion on the need for strong risk analysis skills that can be used to balance business and security challenges.

2011 Advisory Board Meeting Notes

In 2011, the majority of the ISI Advisory Board meeting was spent discussing recommended changes to the MISM Program. The Board unanimously recommended that Ferris modify its graduate program offerings to build on the success and relevance of its undergraduate Information Security & Intelligence Program. As a result of this recommendation, the new MISI program is being introduced this year. Although minimal discussion was spent on the ISI undergraduate program, there were recommendations of new areas of value to them as employers including increased homeland security and intelligence focus, compliance and risk management, and secure software development. As a result of this recommendation, one new National Security Concentration is being introduced in Fall 2012 and a new Secure Software

Development Concentration is planned for Spring 2013. A Concentration focused on policies, compliance and risk management is under consideration.

SECTION 3: PROGRAM PROFILE

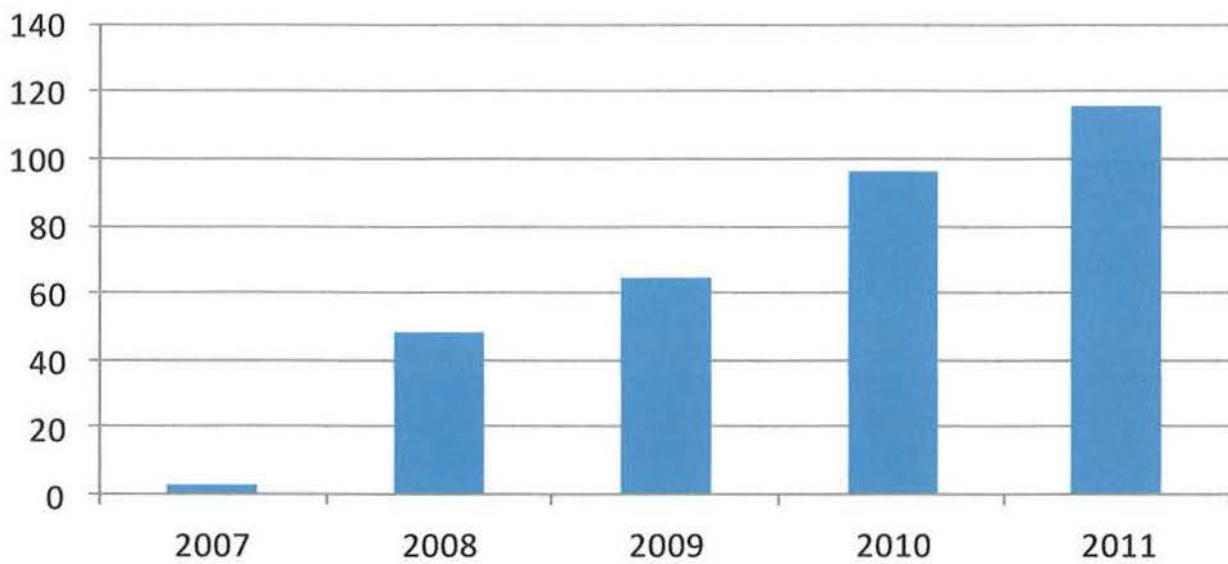
A. ENROLLMENT

As presented in the charts below, the ISI program has grown from 3 students at its start in the Spring of 2007 at the Grand Rapids Campus to 116 students at 4 campus locations (Grand Rapids, Traverse City, Big Rapids and Delta) in 2011.

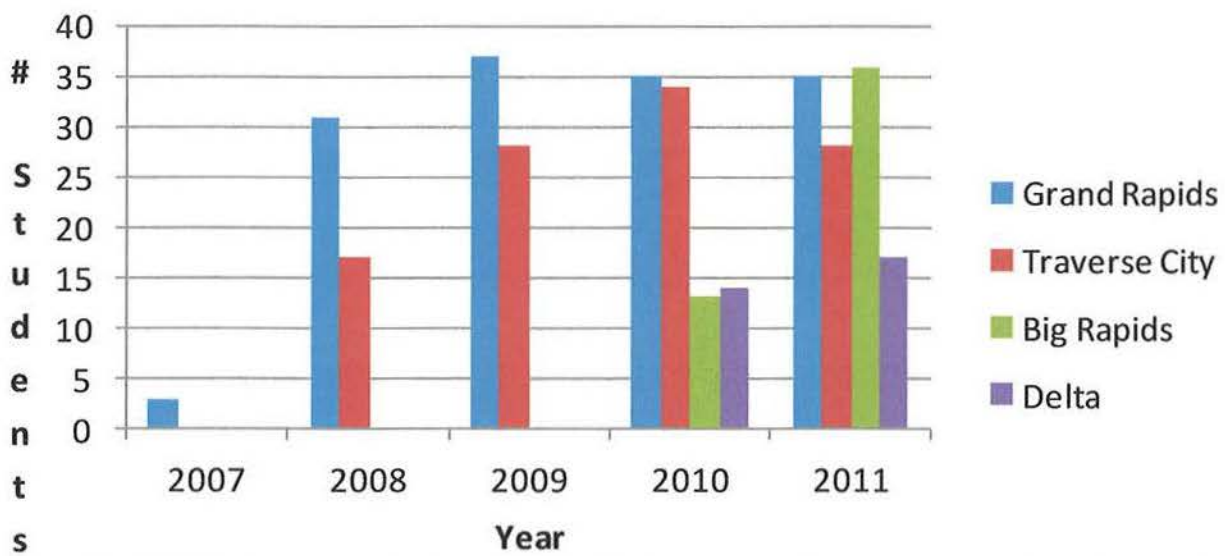
- 2007 to 2008 - 1500% Increase
- 2008 to 2009 - 35% Increase
- 2009 to 2010 – 48% Increase
- 2010 to 2011 – 13% Increase

This demonstrates continued growth in student enrollment since its start in 2007 with predicted 2012 growth continuing at each campus location and the addition of 2 new campuses (Lansing and Harper Woods) in Fall 2012. The goal of the ISI Program is to maintain a minimum of a 10% increase at each current campus location. The additional locations scheduled for roll out in Fall of 2012 (Lansing and Wayne County) will add overall to the growth of the program as well. The *Serving the Military – ISI Online* offering will be available in the Fall of 2013 and is expected to draw a significant student enrollment from activity and veteran military members.

ISI Enrollment 2007 to 2011



ISI Enrollment by Campus Location



B. QUALITY OF CURRICULUM AND INSTRUCTION

The ISI curriculum has been certified as a Center of Excellence by the National Security Agency, Department of Defense and Department of Homeland Security which provides an independent avenue to confirm quality of curriculum and instruction external to Ferris State. The process of achieving this designation involved two steps. The first step required the mapping of the ISI courses to the CNSS standards developed by the NSA which are considered the highest level and most detailed requirements for academic institutions to determine if their curriculum provides appropriate education in information security. The mapping involved over 9,000 individual entries and resulted in the ISI program mapping to all 6 of the CNSS Standards. **Only 8 other institutions in the United States had mapped to all standards.** After receiving notice of our mapping success, the ISI Program was invited to provide further information about the program and faculty including student research samples, faculty CV's, publications and research, as well as University Support for the Program. As a result of this second submission, the ISI Program was designated as a Center of Academic Excellence in Information Assurance Education. The complete result of the CNSS mapping is included at Attachment G.

Although this external vetting of our program is important, student evaluations of our course content and delivery is equally important. The data on this element comes from two sources: Student and alumni survey data and SAI data. In both the student and alumni surveys, the majority of both current students and alumni considered the ISI course content and delivery to be of quality rated as equal to or above 2.5 on a 4 point scale as indicated by their survey results. In examining these results there certainly are areas for improvement and the ISI faculty are committed to continuous improvement in both course content and course delivery. On a classroom basis, it is important to note that the average SAI score across the curriculum and faculty averages between 4.3 and 4.4 each semester. This measure indicates that course content and instruction is quite strong from the student perspective.

The ISI curriculum reflects the current challenges in information security & intelligence, including security fundamentals, forensics, visual analysis, data (database and data

mining), competitive intelligence, risk analysis, fraud, legal and ethical issues, project management, and current issues in information security. (Course Syllabi are included as Attachment C). The Concentrations offered to students reflect the various career paths open to them including forensic analysis, network security, national security, and project management.

All ISI courses are supported and/or delivered via FerrisConnect. The ISI program continues to integrate technology to support instruction into the curriculum including the use of cloud computing lab environments, podcasting, student personal web pages, and video conferencing. The ISI curriculum is also supported by several academic alliances including the Microsoft Academic Alliance, Oracle, VMware, and several other technologies.

C. COMPOSITION AND QUALITY OF THE FACULTY

The composition and quality of the faculty teaching in the ISI program is strong. The ISI faculty members are committed to ongoing improvement in their course delivery and pedagogy as indicated by their attendance at Faculty Center for Teaching and Learning classes each year. The faculty members also have multiple current certifications in the areas they teach including 3 members who have earned the CISSP (Certified Information System Security Professional) designation, 3 members who have earned the PMP (Project Management Professional) designation, one with the CSSLP (Certified System Security Lifecycle Professional) and one a Certified Forensic Encase Examiner. One faculty member was the 2011 FSU Distinguished Teacher.

Each ISI faculty member has published a book, chapter, and/or journal article in both the 2009/2010 and 2010/2011 academic years, as well as given at least one presentation at a conference. In the past 2 years, 3 referred journal articles and 2 books have been published, as well as contributed chapters for additional books which are scheduled to be published in 2012.

Three of the current four full time faculty members of the ISI program have earned their PhD degrees. An additional new faculty member joining the department in Fall of 2012 also comes with a PhD.

The ISI Program occasionally relies on adjunct assistance. Adjunct faculty who teach ISI courses must meet the same stringent academic, experience and certification experience required from full time faculty teaching the course. Additional adjunct faculty members are being recruited to support our continuing growth in offering the program in various locations throughout Michigan.

Another measure of faculty quality is initiatives taken in areas such as grant writing. The ISI faculty members have been successful writing a grant from the Ferris Foundation, and also have received a \$450,000 grant by the National Science Foundation for research in forensic analysis using electron microscopy. Members of the ISI faculty have also submitted grants to the Department of Justice and three other non-funded NSF requests since 2009 and responding to grant offerings is a high priority goal of the program.

All ISI faculty members consult with organizations to remain current in the field, including areas of information security, national security, intelligence, project management, database, and risk management. Additionally, two faculty members have taught adjunct at the University of West Virginia, Norwich University, Excelsior College and the University of Maryland to develop an understanding of how similar programs are run at other academic institutions.

Faculty vitas are included as Attachment B to this report.

SECTION 4: FACILITIES AND EQUIPMENT

An important goal of the ISI program is to provide hands-on experience with best-in-class information security and intelligence technology. To that end, the ISI Program has established educational partnerships with the following providers of specialized technology and software.

- Access Data EnCase Forensic Software
- IBM I2 Visual Analysis Software
- Paraben Mobile Forensic Technology
- THREADS Mobile Forensic Technology
- Cellebrite Mobile Forensic Technology

All ISI students have access to the MSDN Alliance and use the various Microsoft products including Office, Visio and Project in their course work.

Additionally, ISI courses use OpenSource technology including:

- MySQL database
- BackTrack5 which is a suite of ethical hacking tools and technologies

All software and technology tools are made available to students as part of their course experience either through cloud based delivery, lab environments, or student installations of software on their computers.

As the ISI program continues to grow, there is a need for further investment in these technology tools including an increase in licensing for concurrent use and additional units for mobile forensic investigation. Additionally as new technology becomes available for information security and intelligence investigations, it is essential that the ISI program remain in the forefront in providing hands on training in these tools to its students.

The ISI Program is also served by FLITE (Ferris Library for Information, Technology, and Education) which provides students access to current research in information security and intelligence through its databases and research resources. FLITE has assigned a designated research librarian to assist COB programs including ISI.

The ISI program is supported by the administrative and student support team at each campus location. Students report high levels of responsiveness and assistance to their questions and concerns by administrative staff members. Academic advising is conducted by the ISI faculty members and students and alumni report high levels of satisfaction with the academic advisory services they received.

Ferris Connect and Ferris Learn are essential components in ISI course delivery. All ISI courses are either hybrid or online which allows for increased convenience for students as well as improved handling of assignments, assessments, discussions, and grading. In addition to online course delivery, the ISI program is committed to meeting the Ferris Quality Matters Standards in its course design and development. All ISI courses will be converted to the Ferris Learn environment no later than December 2012. Additionally, as discussed earlier, the ISI program is increasing its use of the SkyTap cloud environment to providing laboratory environments for students to use at their convenience.

SECTION 5: CONCLUSIONS

The Information Security & Intelligence Program has experienced continued growth in enrollment since it began in the spring of 2007. The success of the program is credited to the uniqueness and distinctiveness of its course offerings as well as its relevance to the increasing demands for information security professionals. Continued growth in enrollment is predicted as the program draws more students to its current campus locations and expands to new campuses. Although campus growth is not expected to continue at the same pace as has occurred between 2007 and 2011, the entry of the *Serving the Military – ISI Online* program in Fall of 2013 is expected to be very successful based upon conversations with various military representatives.

Challenges

Although there are increasing numbers of information security jobs available, many of them require experience in the field. The ISI Program needs to have greater emphasis on internships for its students. For those students with little or no prior experience, multiple internships would be beneficial in preparing themselves to enter the full time information security profession.

Although the growth of the ISI program is positive and seen as a confirmation of its relevance, it brings several risks as well. As the need to deliver more course offerings, the ISI program must increase its use of adjunct faculty. In order to ensure high quality and consistency, the ISI Program will establish a process of monitoring, coaching, and content course review for all new adjunct faculty members. There is also a risk that the program would lose its relevance if its course content does not remain current with evolving information security challenges. The growing emphasis on research activities along with continued emphasis on publications and conference presentations should help alleviate some of this risk.

Lastly, although the ISI program is one of the few undergraduate programs offering degrees in information security, the competition can only be expected to grow as this

field becomes one of high demand. The ISI faculty members are committed to maintaining high quality, relevance and innovation in its course offerings as its best antidote to competition. However, that commitment may not be enough. The ISI Program will also need to better market its offerings both in targeting online and traditional marketing campaigns. Sponsorship of information security conferences such as GrrCONN, Infragard and SecureWorld are recommended ways to expand ISI brand awareness and reputation.

Incomplete Institutional Data

Although we have successfully mapped to the external criteria established by the National Security Agency, as demonstrated by the attached TracDat reports, the ISI Program is not current with the institutional tracking of program and course objectives and assessment methodologies. This is an area that requires immediate attention and will be addressed by the ISI faculty who will commit to updating all TracDat data no later than October 31, 2012.

ISI SWOT Analysis

In 2011 the College of Business Strategic Planning Process required each Program to develop a SWOT analysis that would identify their specific Strengths, Weaknesses, Opportunities and Threats. Based on the SWOT analysis, which is included as Attachment F, below is the list of ISI Program goals for the 2012 academic year in order of priority.

- Expansion of ISI program to other locations.
- Increase enrollment by 20% at each program location
- Work with new International Education Center to develop strong global partnerships with other universities around the world that results in faculty and student exchanges.
- Increase international enrollment in program.
- Work with New Incubator initiative to develop innovative new programs and opportunities.

- Develop marketing materials and plan marketing events to inform and promote the ISI program throughout Michigan.
- Develop Special Topic courses, seminars and conferences on topics identified by our Advisory Board including Business Intelligence, Mobile and Cloud Computing, Database and Database Security, Secure Application Development, Privacy, Risk, Compliance and Governance; and expand focus to encompass national and corporate security
- Work with new Grant Office to pursue grants through NSA and other funding sources
- Build strong student organization (ISIA)
- Achieve Quality Matters certification for online and hybrid courses
- Build strong diverse adjunct base to support expansion of program
- Partner with various organizations such as ISSA, Automation Alley, ISACA and with communities to professional networking and service learning opportunities for students

Benefit to Ferris State University

One of the most important questions to answer as part of the Academic Program Review process is whether the Program brings value and benefits to Ferris State University as a higher education academic institution in Michigan. The ISI Program Faculty members believe that the ISI Program brings the following value and benefits to Ferris State University:

- Midwest recognition of the quality of the ISI Program through its partnerships with community colleges, professional organizations, intelligence and law enforcement agencies.
- National recognition of the quality of the ISI Program content through its designation as a Center of Academic Excellence in Information Security Education.

- National recognition of forensic expertise resulting from the \$450,000 NSF Grant for forensic research utilizing electron microscopy.
- International recognition of ISI faculty members due to their publications, research and other collaborations with co-authors and collaborators throughout the world.
- An undergraduate program that demonstrates continual increase and expansion in course offerings and student enrollments.
- A highly committed and innovative faculty team who demonstrate their commitment to continuous improvement through their annual review of courses that result in appropriate additions and changes to the curriculum as needed based on input from the ISI Advisory Board and experts in the field of Information Security & Intelligence.

Appendices

Appendix A: Surveys

Current Student Survey Results

1. How do you feel about the quality of the content of the courses required by the ISIN program?

	Poor	Neutral	Average	Exceptional	Rating Average	Response Count
All Things Digital	6.7% (2)	13.3% (4)	30.0% (9)	50.0% (15)	3.23	30
Introduction to Information Security	0.0% (0)	14.3% (4)	28.6% (8)	57.1% (16)	3.43	28
Data Mining	18.2% (4)	40.9% (9)	18.2% (4)	22.7% (5)	2.45	22
Risk Analysis	9.1% (2)	36.4% (8)	18.2% (4)	36.4% (8)	2.82	22
Digital Forensics	3.6% (1)	14.3% (4)	21.4% (6)	60.7% (17)	3.39	28
Project Management	0.0% (0)	30.4% (7)	39.1% (9)	30.4% (7)	3.00	23
GIS	17.4% (4)	30.4% (7)	30.4% (7)	21.7% (5)	2.57	23
Visual Analysis	0.0% (0)	41.7% (10)	12.5% (3)	45.8% (11)	3.04	24
Data Intelligence Competitive Theory	0.0% (0)	45.8% (11)	16.7% (4)	37.5% (9)	2.92	24
Fraud Examination	7.1% (2)	25.0% (7)	17.9% (5)	50.0% (14)	3.11	28
Legal and Ethical Issues	0.0% (0)	37.5% (9)	12.5% (3)	50.0% (12)	3.13	24
Database Design	4.5% (1)	50.0% (11)	18.2% (4)	27.3% (6)	2.68	22
Applications of Information Security	0.0% (0)	37.5% (9)	16.7% (4)	45.8% (11)	3.08	24
					Comments	9
					answered question	31
					skipped question	0

2. How do you feel about the faculty instruction and delivery of the courses in the ISIN program?

	Poor	Neutral	Average	Exceptional	Rating Average	Response Count
All Things Digital	3.3% (1)	16.7% (5)	23.3% (7)	56.7% (17)	3.33	30
Principles of Information Security	0.0% (0)	17.2% (5)	17.2% (5)	65.5% (19)	3.48	29
Data Mining	13.0% (3)	34.8% (8)	21.7% (5)	30.4% (7)	2.70	23
Risk Analysis	4.2% (1)	37.5% (9)	16.7% (4)	41.7% (10)	2.96	24
Database Design	9.1% (2)	36.4% (8)	22.7% (5)	31.8% (7)	2.77	22
Digital Forensics	3.6% (1)	14.3% (4)	17.9% (5)	64.3% (18)	3.43	28
Visual Analysis	0.0% (0)	37.5% (9)	16.7% (4)	45.8% (11)	3.08	24
Data Intelligence Competitive Theory	0.0% (0)	43.5% (10)	13.0% (3)	43.5% (10)	3.00	23
Project Management	0.0% (0)	37.5% (9)	29.2% (7)	33.3% (8)	2.96	24
Fraud Examination	3.7% (1)	33.3% (9)	11.1% (3)	51.9% (14)	3.11	27
Legal and Ethical Issues	0.0% (0)	40.0% (10)	12.0% (3)	48.0% (12)	3.08	25
Applications of Information Security	0.0% (0)	40.0% (10)	12.0% (3)	48.0% (12)	3.08	25
					Comments	9
					answered question	30
					skipped question	1



3. How do you feel about the relevance of the concentrations offered in the ISIN program?

	Not relevant	Somewhat relevant	Relevant	Very relevant	Rating Average	Response Count
Digital Forensics	0.0% (0)	0.0% (0)	26.7% (8)	73.3% (22)	3.73	30
Network Security	0.0% (0)	3.4% (1)	10.3% (3)	86.2% (25)	3.83	29
Foreign Language	10.7% (3)	28.6% (8)	39.3% (11)	21.4% (6)	2.71	28
National Security (Fall 12)	0.0% (0)	3.8% (1)	26.9% (7)	69.2% (18)	3.65	26
Secure Software Development (Spring 13)	0.0% (0)	3.7% (1)	33.3% (9)	63.0% (17)	3.59	27
GIS and Data Mining	7.1% (2)	28.6% (8)	32.1% (9)	32.1% (9)	2.89	28
					Comments	3
					answered question	30
					skipped question	1





4. The ISIN program provides me with enough background in Information Security and Intelligence to confidently seek employment in a related field.

		Response Percent	Response Count
Strongly Disagree		3.2%	1
Disagree		16.1%	5
Neutral		22.6%	7
Agree		64.5%	20
		Comments	6
		answered question	31
		skipped question	0

5. The academic advising that I receive from ISIN faculty is accurate and helpful.

		Response Percent	Response Count
Strongly Disagree		6.5%	2
Disagree		0.0%	0
Neutral		16.1%	5
Agree		77.4%	24
	Comments		5
	answered question		31
	skipped question		0





6. I am generally well satisfied with the ISI curriculum.

		Response Percent	Response Count
Strongly Disagree		3.3%	1
Disagree		0.0%	0
Neutral		13.3%	4
Agree		40.0%	12
Strongly Agree		43.3%	13
	Comments		3
	answered question		30
	skipped question		1

7. Please indicate your preferred approaches to course offerings?

	Not Preferred	Neutral	Preferred	Rating Average	Response Count
Completely Online	20.0% (6)	36.7% (11)	43.3% (13)	2.23	30
Completely Face-to-Face Classroom	33.3% (9)	33.3% (9)	33.3% (9)	2.00	27
Hybrid Mix Classroom (1 day/week) and Online for 7 weeks	10.7% (3)	14.3% (4)	75.0% (21)	2.64	28
Hybrid Mix Classroom (1 day/week) and online for 15 weeks	17.2% (5)	24.1% (7)	58.6% (17)	2.41	29
Weekends	55.6% (15)	33.3% (9)	11.1% (3)	1.56	27
				Comments	5
				answered question	31
				skipped question	0



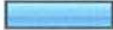


8. I feel that in general the ISIN courses are intellectually challenging.

		Response Percent	Response Count
Strongly Disagree		0.0%	0
Disagree		9.7%	3
Neutral		12.9%	4
Agree		51.6%	16
Strongly Agree		29.0%	9
		Comments	5
		answered question	31
		skipped question	0

9. There is a feeling of camaraderie (friendliness) in the ISIN program among students and faculty.


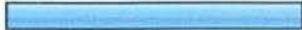


		Response Percent	Response Count
Strongly Disagree		3.2%	1
Disagree		0.0%	0
Neutral		12.9%	4
Agree		32.3%	10
Strongly Agree		51.6%	16
	Comments		0
	answered question		31
	skipped question		0

10. I feel that the technology resources used in the ISIN program are adequate and reliable.





		Response Percent	Response Count
Strongly Disagree		6.5%	2
Disagree		3.2%	1
Neutral		16.1%	5
Agree		38.7%	12
Strongly Agree		35.5%	11
	Comments		3
	answered question		31
	skipped question		0

Alumni Survey Results




1. In what year did you enter the ISIN program?

		Response Percent	Response Count
2007		27.3%	3
2008		45.5%	5
2009		18.2%	2
2010		9.1%	1
2011		0.0%	0
2012		0.0%	0
answered question			11
skipped question			0

2. In what year did you graduate or leave the ISIN program?

		Response Percent	Response Count
2007		0.0%	0
2008		0.0%	0
2009		9.1%	1
2010		45.5%	5
2011		18.2%	2
2012		9.1%	1
answered question			11
skipped question			0

3. What was the campus location at which you took your ISIN classes?

		Response Percent	Response Count
Big Rapids		27.3%	3
Bay City		0.0%	0
Grand Rapids		63.6%	7
Traverse City		27.3%	3
		answered question	11
		skipped question	0

4. While a student in the ISIN program, how did you feel about the quality of the content of the courses required by the ISIN program?

	Poor	Neutral	Average	Exceptional	Rating Average	Response Count
All Things Digital	0.0% (0)	18.2% (2)	54.5% (6)	27.3% (3)	3.09	11
Introduction to Information Security	0.0% (0)	0.0% (0)	55.6% (5)	44.4% (4)	3.44	9
Data Mining	18.2% (2)	45.5% (5)	9.1% (1)	27.3% (3)	2.45	11
Risk Analysis	27.3% (3)	27.3% (3)	36.4% (4)	9.1% (1)	2.27	11
Digital Forensics	0.0% (0)	0.0% (0)	9.1% (1)	90.9% (10)	3.91	11
Project Management	0.0% (0)	10.0% (1)	30.0% (3)	60.0% (6)	3.50	10
GIS	18.2% (2)	27.3% (3)	36.4% (4)	18.2% (2)	2.55	11
Visual Analysis	0.0% (0)	9.1% (1)	9.1% (1)	81.8% (9)	3.73	11
Data Intelligence Competitive Theory	0.0% (0)	18.2% (2)	18.2% (2)	63.6% (7)	3.45	11
Fraud Examination	0.0% (0)	9.1% (1)	18.2% (2)	72.7% (8)	3.64	11
Legal and Ethical Issues	0.0% (0)	30.0% (3)	10.0% (1)	60.0% (6)	3.30	10
Database Design	10.0% (1)	20.0% (2)	20.0% (2)	50.0% (5)	3.10	10
Applications of Information Security	0.0% (0)	22.2% (2)	22.2% (2)	55.6% (5)	3.33	9
				Comments		5
				answered question		11
				skipped question		0





5. While a student in the ISIN program, how did you feel about the faculty instruction and delivery of the courses in the ISIN program?

	Poor	Neutral	Average	Exceptional	Rating Average	Response Count
All Things Digital	0.0% (0)	9.1% (1)	36.4% (4)	54.5% (6)	3.45	11
Principles of Information Security	0.0% (0)	10.0% (1)	20.0% (2)	70.0% (7)	3.60	10
Data Mining	45.5% (5)	18.2% (2)	0.0% (0)	36.4% (4)	2.27	11
Risk Analysis	27.3% (3)	36.4% (4)	18.2% (2)	18.2% (2)	2.27	11
Database Design	10.0% (1)	30.0% (3)	10.0% (1)	50.0% (5)	3.00	10
Digital Forensics	0.0% (0)	0.0% (0)	0.0% (0)	100.0% (11)	4.00	11
Visual Analysis	0.0% (0)	0.0% (0)	9.1% (1)	90.9% (10)	3.91	11
Data Intelligence Competitive Theory	0.0% (0)	18.2% (2)	18.2% (2)	63.6% (7)	3.45	11
Project Management	0.0% (0)	20.0% (2)	10.0% (1)	70.0% (7)	3.50	10
Fraud Examination	0.0% (0)	18.2% (2)	27.3% (3)	54.5% (6)	3.36	11
Legal and Ethical Issues	0.0% (0)	30.0% (3)	10.0% (1)	60.0% (6)	3.30	10
Applications of Information Security	0.0% (0)	30.0% (3)	30.0% (3)	40.0% (4)	3.10	10
					Comments	2
					answered question	11
					skipped question	0



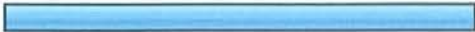
6. As an alumni of the ISIN program, how relevant are the concentrations offered in the ISIN program?

	Not relevant	Somewhat relevant	Relevant	Very relevant	Rating Average	Response Count
Digital Forensics	0.0% (0)	9.1% (1)	27.3% (3)	63.6% (7)	3.55	11
Network Security	0.0% (0)	9.1% (1)	18.2% (2)	72.7% (8)	3.64	11
Foreign Language	9.1% (1)	72.7% (8)	9.1% (1)	9.1% (1)	2.18	11
National Security (Fall 12)	22.2% (2)	22.2% (2)	33.3% (3)	22.2% (2)	2.56	9
Secure Software Development (Spring 13)	30.0% (3)	10.0% (1)	20.0% (2)	40.0% (4)	2.70	10
GIS and Data Mining	10.0% (1)	40.0% (4)	30.0% (3)	20.0% (2)	2.60	10
				Comments		3
				answered question		11
				skipped question		0




7. The ISIN program provided you with enough education and skills in Information Security and Intelligence to achieve employment in the ISIN field of your choice

		Response Percent	Response Count
Strongly Disagree		9.1%	1
Disagree		27.3%	3
Neutral		9.1%	1
Agree		54.5%	6
		Comments	3
		answered question	11
		skipped question	0



8. The academic advising that I received from ISIN faculty was accurate and helpful.

		Response Percent	Response Count
Strongly Disagree		9.1%	1
Disagree		0.0%	0
Neutral		18.2%	2
Agree		72.7%	8
		Comments	3
		answered question	11
		skipped question	0




9. The ISIN program contributed in a positive manner to my ability to problem solve, work on a team, and communicate verbally and in a written format.

		Response Percent	Response Count
Strongly Disagree		0.0%	0
Disagree		0.0%	0
Neutral		9.1%	1
Agree		27.3%	3
Strongly Agree		63.6%	7
		Comments	2
		answered question	11
		skipped question	0



10. If you could go back and start over, would you choose the Ferris State ISI Program again?

		Response Percent	Response Count
Yes		80.0%	8
No		20.0%	2
	Comments		6
	answered question		10
	skipped question		1



11. While a student in the ISIN program, I felt that in general the ISIN courses are intellectually challenging.

		Response Percent	Response Count
Strongly Disagree		0.0%	0
Disagree		0.0%	0
Neutral		9.1%	1
Agree		54.5%	6
Strongly Agree		36.4%	4
	Comments		1
	answered question		11
	skipped question		0




12. While a student in the ISIN program, there is a feeling of camaraderie (friendliness) in the ISIN program among students and faculty.

		Response Percent	Response Count
Strongly Disagree		0.0%	0
Disagree		0.0%	0
Neutral		0.0%	0
Agree		27.3%	3
Strongly Agree		72.7%	8
	Comments		4
	answered question		11
	skipped question		0

13. How long after leaving the ISI Program did it take to find employment?

		Response Percent	Response Count
Pre-employed		45.5%	5
0-6 months		27.3%	3
7-11 months		0.0%	0
12-17 months		0.0%	0
18-21 months		0.0%	0
Never		9.1%	1
Continued Education		18.2%	2
	answered question		11
	skipped question		0



14. What is your current income range? (U.S. dollars)

		Response Percent	Response Count
Under \$20,000		0.0%	0
\$20,000-\$35,000		0.0%	0
\$35,001-\$50,000		40.0%	4
\$50,001-\$70,000		40.0%	4
\$70,001-\$85,000		20.0%	2
Over \$85,001		0.0%	0
answered question			10
skipped question			1



15. The faculty in the ISIN program cared about my progress.

		Response Percent	Response Count
Yes		100.0%	10
No		0.0%	0
answered question			10
skipped question			1

16. I am employed in my major or a closely related field.

		Response Percent	Response Count
Yes		70.0%	7
No		30.0%	3
	Comments		3
	answered question		10
	skipped question		1

17. Would you recommend the ISIN program to others?

		Response Percent	Response Count
Yes		90.0%	9
No		10.0%	1
	Comments		2
	answered question		10
	skipped question		1

Q4. While a student in the ISIN program, how did you feel about the quality of the content of the courses required by the ISIN program?

1	Some of the classes above were either not offered or I wasn't required to take at the time I was enrolled, so I have not ranked them. The classes that I ranked poor were basically all theory and no application and what application was portrayed was not even close to the ISIN program's subject matter.	May 14, 2012 9:14 AM
2	All of the core ISI courses were great. The only lower quality courses were outlying departments, in my opinion.	May 5, 2012 1:08 AM
3	Risk Analysis - I had Nate Tymes for this class and it seemingly was not well organized and also did not incorporate elements of information security.	May 2, 2012 12:26 PM
4	My first Risk Analysis class I felt had nothing to do with Info Sec and all to do with Math. That was so disappointing because I had to retake it :(With someone different who did cover Info Sec application to Risk Analysis. GIS was another very difficult class taking it online. This is a class that needs to be "In Class". The first class totally turned me off to this area of Info Sec and that isn't what it is suppose to do. Another class I had that was terrible was Business Writing which the teacher disappeared half way through the class. Other than these 3 classes all the rest were good. The other comment I want to make is that there needs to be emphasis on Securing Networks for business. I had none of that and that is HUGE. Why not??	May 2, 2012 6:45 AM
5	The DF and visual analysis classes were outstanding.	May 2, 2012 5:53 AM

Q5. While a student in the ISIN program, how did you feel about the faculty instruction and delivery of the courses in the ISIN program?

1	Data Mining: Elies Kouider Risk Analysis: Nate Tymes Database Design: Warner Myntti	May 2, 2012 12:26 PM
2	Those checked neutral are because I took those through community college and don't apply here. The other 2 poor are also noted in my comments above.	May 2, 2012 6:45 AM

Q6. As an alumni of the ISIN program, how relevant are the concentrations offered in the ISIN program?

1	More so Data Mining for me in the business world.	May 2, 2012 12:26 PM
2	I don't recall any Network Security but it needs to be there.	May 2, 2012 6:45 AM
3	I am currently employed in the National Security, Federal Criminal Investigations area.	May 2, 2012 5:53 AM

Q7. The ISIN program provided you with enough education and skills in Information Security and Intelligence to achieve employment in the ISIN field of your choice

1	I am working now in the field that I worked in before going back to school at Ferris, much to my dismay. This is only due to the fact that I could not find a position in information security research, digital forensics or intelligence. When enrolling in the program as well as during the time I was in it I was led to believe that I would be able to obtain a position in this field around the GR area. After graduation the only help I got was to say that I might be able to get a job at an insurance company and not even in GR. I was also led to believe that I would be able to keep a position with SAIC (this was a company I did an internship with) to work on future projects, this dried up as well, incidentally, I quit my job to take this internship. To my knowledge my work was above average and I got along well with other students and the faculty as well. My grades were above average as I graduated Summa cum laude. So for me I feel that I wasted two years of my life, a lot of money including all of my savings and retirement due to my internship with SAIC being over at a time when the unemployment was at its highest here in Michigan. Also, I did have an interview for an Information Security Engineer (Entry Level), where I was embarrassed due to the lack of technical knowledge that I had during the questioning.	May 14, 2012 9:14 AM
2	I am sad to say I don't feel that I am prepared to secure a network for a company and that is something they will expect. I have the basics and have the desire to fill in the gaps so I will make it but for future students they need more emphasis on Network security and preventing and discovering data breeches.	May 2, 2012 6:45 AM
3	The ISIN program provides a good foundational understanding of many different types of employment (forensics, national security, counter-intelligence, information assurance, etc)	May 2, 2012 5:53 AM

Q8. The academic advising that I received from ISIN faculty was accurate and helpful.

1	See #7	May 14, 2012 9:14 AM
2	I was so fortunate to have the best!!	May 2, 2012 6:45 AM
3	Dr. Gogolin and Bob Ewigleben were excellent mentors	May 2, 2012 5:53 AM

Q9. The ISIN program contributed in a positive manner to my ability to problem solve, work on a team, and communicate verbally and in a written format.

1	As I had been in the workforce for over twenty years prior to enrolling in the ISIN program I feel that I had a pretty good handle on the above abilities.	May 14, 2012 9:14 AM
2	Absolutely	May 2, 2012 6:45 AM

Q10. If you could go back and start over, would you choose the Ferris State ISI Program again?

1	See #7	May 14, 2012 9:14 AM
2	Absolutely	May 5, 2012 1:08 AM
3	Cis or computer science because that is more what I am interested in	May 4, 2012 2:27 PM
4	Typo, this should be ISIN not ISM. Maybe I would have picked that one though!	May 2, 2012 12:26 PM
5	I didn't got through the ISM program ?? ISI yes	May 2, 2012 6:45 AM
6	It seems that it is only getting better as time goes on. I would love to be an ISIN instructor at some point in my career.	May 2, 2012 5:53 AM

Q11. While a student in the ISIN program, I felt that in general the ISIN courses are intellectually challenging.

1	Yes	May 2, 2012 6:45 AM
---	-----	---------------------

Q12. While a student in the ISIN program, there is a feeling of camaraderie (friendliness) in the ISIN program among students and faculty.

1	ISIN students congregated together in non ISIN courses. I also noticed a caliber difference in ISIN versus CIS majors.	May 5, 2012 1:08 AM
2	Typo in #13	May 2, 2012 12:26 PM
3	Very much so	May 2, 2012 6:45 AM
4	When I went through, we were the 'test gerbils', so we had a bond that derived from our common goal of getting our degree at (near) the same time.	May 2, 2012 5:53 AM

Q16. I am employed in my major or a closely related field.


1	See #7. Comment for #15 - I feel they cared while enrolled but once graduated, they really didn't care.	May 14, 2012 9:14 AM
2	Software development but have used forensics skills for PADSS certification	May 4, 2012 2:27 PM
3	Continuing education	May 2, 2012 6:45 AM

Q17. Would you recommend the ISIN program to others?

- | | | |
|---|---|-----------------------|
| 1 | I'd have to really see what there interests are first.Other degrees might fit well | May 12, 2012 10:48 AM |
| 2 | I would but there does need to be improvement in some of the classes I noted above. | May 2, 2012 6:45 AM |

COB Faculty Survey Results




1. In which College do you currently teach?

		Response Percent	Response Count
Allied Health		0.0%	0
Arts and Sciences		0.0%	0
Business		100.0%	18
Education and Human Services		0.0%	0
Engineering Technology		0.0%	0
Extended and International		0.0%	0
Kendall		0.0%	0
Pharmacy		0.0%	0
Optometry		0.0%	0
University College		0.0%	0
answered question			18
skipped question			0




2. Are you aware of the Information Security & Intelligence program in the College of Business?

		Response Percent	Response Count
Yes		94.4%	17
No		5.6%	1
answered question			18
skipped question			0




3. What is your perception of the quality of course content presented in the Information Security & Intelligence Program?

		Response Percent	Response Count
Poor		5.6%	1
Neutral		0.0%	0
Average		22.2%	4
High		72.2%	13
answered question			18
skipped question			0

4. What is your perception of the relevance of the Information Security & Intelligence program to students looking for professional careers?

		Response Percent	Response Count
Poor		0.0%	0
Neutral		5.6%	1
Average		5.6%	1
High		88.9%	16
answered question			18
skipped question			0



5. What is your perception of the quality of instruction in the Information Security & Intelligence program?

		Response Percent	Response Count
Poor		0.0%	0
Neutral		5.6%	1
Average		33.3%	6
High		61.1%	11
answered question			18
skipped question			0

6. What recommendations do you have for improving the Information Security & Intelligence program?

	Response Count
	3
answered question	3
skipped question	15

7. Would you like to learn more about the Information Security & Intelligence program?

		Response Percent	Response Count
Yes		23.5%	4
No		76.5%	13
answered question			17
skipped question			1

8. Are there opportunities for collaboration between your program and the Information Security & Intelligence program?

	Response Count
	5
answered question	5
skipped question	13

Q6. What recommendations do you have for improving the Information Security & Intelligence program?

1	more marketing, as faculty member in the same college, not sure of where the graduates are going, and do not know that much about the program.	May 2, 2012 11:03 AM
2	Since I am not in the area my opinions are worth as much as the paper on which this survey is written. Hey wait, this is not written on paper. My point exactly.	May 2, 2012 10:42 AM
3	Incorporate more software development and design courses with a focus on security	May 2, 2012 6:13 AM

Q8. Are there opportunities for collaboration between your program and the Information Security & Intelligence program?

1	Perhaps	May 7, 2012 12:01 PM
2	I'm sure there would be.	May 2, 2012 11:03 AM
3	Probably, but who the hell has the time? We are kept busy doing a lot of administrative busy work such as the APR. If I had some time, I would improve the teaching of my own courses and I would meet with potential employers so that I could help my students get jobs. Sadly teaching and employment no longer seem to be priorities at FERRIS. Just get those surveys done. Get those APR's done. Get those track dats done so that clueless people like our dean can say, "I am all bout accountability." Who's job is it to keep this Bozo accountable? The next time I walk by his office and he is sitting with his legs on his desk with his hands behind his head..In deep thought no doubt..I am going to loose it.	May 2, 2012 10:42 AM
4	perhaps	May 2, 2012 8:18 AM
5	Yes	May 2, 2012 6:09 AM

Appendix B: Faculty Vita

Full Time Faculty

Dr. Doug L. Blakemore

Ferris State University

AFIS

Email: blakemod@ferris.edu

Education

Ph D, Capella University, 2003.

Major: Organization and Management

MS, Ferris State University, 1994.

Major: Information Systems Management

Professional Positions

Professional

Owner/manager, Cornerstone Services. (1982 - Present).

Licensures and Certifications

Certificate in Unix/Linux Administration, University of IL. (2005 - Present).

Certified Dyslexia Instructor, Michigan Dyslexia Institute. (1994 - Present).

Professional Memberships

ACFE.

Infragard. (September 2010 - Present).

Development Activities Attended

Seminar, "Paraben Level 1 certification," Paraben. (May 2010).

Workshop, "I2," I2, Inc. (July 10, 2009 - July 15, 2009).

Conference Attendance, "Symposium on assessment," Univ. of South Carolina. (May 12, 2009 - May 15, 2009).

Workshop, "Encase - Intermediate level training," Guidance Software. (December 10, 2007 - December 15, 2007).

TEACHING

Directed Student Learning

Dissertation Committee Member. (2006).

Advised: Teresa Cook

RESEARCH

Published Intellectual Contributions

Refereed Journal Articles

Blakemore, D. L. (2006). *Adam Smith Review*.

Journal Articles

Blakemore, D. L. (2006). *Academy of Management Review*.

Presentations Given

Blakemore, D. L., Regional Accounting Seminar, "Keynote Presentation," Cadillac, MI. (2007).

Blakemore, D. L., "Solaris Unix for Oracle Managers." (2006).

Blakemore, D. L., Business Seminar, "Basil Linux Configurations," Greenville, MI. (2005).

Blakemore, D. L., Ferris State University AFIS Department, "Turnitin.com," Ferris State University AFIS Department, Big Rapids, MI. (2005).

Blakemore, D. L., Business Seminar, "Microsoft Excel 2000 Advanced Functions for Accounting," Big Rapids, MI. (2004).

Blakemore, D. L., Distance Education Seminar, "Distance Education," Ferris State University AFIS Department, Big Rapids, MI. (2003).

Blakemore, D. L., Y2K Readiness, "Y2K Readiness," Cadillac, MI. (1999).

SERVICE

Department Service

Co-chair, Search Committee. (2006 - 2007).

Committee Member, Academic Program Review Committee. (2004 - 2005).

College Service

Committee Member, Assessment Tracking Committee. (2007 - 2008).

Committee Member, College of Business Promotion Merit Committee. (2006 - 2007).

Committee Chair, College of Business Sabbatical Review Committee. (2005 - 2006).

Committee Member, Search Committee. (2005 - 2006).

University Service

Task Force Member, University Graduate Council. (2005 - 2010).

Committee Member, ECNS Program Review Committee. (2007 - 2008).

Faculty Advisor, Delta Chi. (2005 - 2006).

Committee Member, University Sabbatical Review Committee. (2005 - 2006).

Committee Member, Business/Technology Consortium Advisory Committee. (2002 - 2005).

Professional Service

Editor, Pedagogical, Business Review. (2004 - 2006).

Debate, Ferris State University, Big Rapids, MI. (2004).

Public Service

Officer, Secretary, Pawfect Companions - Therapy Dog association, Big Rapids, MI. (January 1, 2005 - December 31, 2008).

Consulting

Computer Consulting. (1982 - Present).

Mark IV Enterprise. (2005).

Greg E. Gogolin, Ph.D
CISSP, EnCE, PMP, PI
Ferris State University

Education

- Ph D, Michigan State University, 2000.
Major: College and University Administration
Supporting Areas of Emphasis: Instructional Technology
Dissertation Title: "A Case Study of an Approach to Nursing Education using a Mixed Model of Distance and Live Instruction"
- Doctoral Study, NOVA Southeastern Florida, 1999-2000.
Major: Computer Information Systems
Supporting Areas of Emphasis: Human Computer Interaction
- MS, Ferris State University, 1991.
Major: Computer Information Systems Management
Dissertation Title: "An Evaluation of CASE Technology compared to traditional Third-Generation Development Methodologies"
- BS, Ferris State University, 1987.
Major: Applied Biology
- BS, Ferris State University, 1987.
Major: Computer Information Systems
- AA, Ferris State University, 1983.
Major: Arts

Certifications & License

- Private Investigator, State of Michigan, License # 3701-205799
- CISSP, Certified Information Systems Security Professional, 2009 – present.
Information Systems Security Certification Consortium (ISC2)
- PMP, Project Management Professional, 2004 - present.
Project Management Institute
- EnCE, Certified EnCase Examiner (Digital Forensics), 2008 - present.
Guidance Software
- Certified Handheld Examiner (Digital Forensics), 2009 - present.
Paraben

Professional Positions

Professional

- Professor, Ferris State University, Big Rapids, MI 49307. (1999-present).
- Professional Investigator/Consultant, Rockford Files, LLC. (2001-present).
- Systems Analyst, Database Administrator, Project Manager, Amway Corporation. (1991 - 1999).
- Computer Programmer, Senior Analyst/Programmer, Gerber Products. (1987 - 1991).
- Computer Programmer, Advanced Systems Applications. (1987).

Retail Store Manager, computer programmer, ShortStop, Inc. (1984 - 1987).
Yoplait, USA., computer programmer - inventory management. (1981, 1982).

Development Activities Attended

Readings.
Website visitation/subscriber.
Workshops. (1991 - Present).
Workshop, "PresentationZen," Ferris Center for Teaching & Learning. (Fall 2010).
Workshop, "Rubrics, Readability, and Retention," Ferris Center for Teaching & Learning. (Fall 2010).
Seminar, "Paraben Cell Phone/Handheld Forensics training." (May 2009).
Seminar, "EnCase Advanced Computer Forensics training." (April 2009).
Seminar, "EnCase EnCE examination training." (July 2008).
Seminar, "EnCase Computer Forensics II training." (June 2008).
Seminar, "EnCase Computer Forensics I training." (May 2008).
Workshop, "Course Portfolio Workshop," Ferris Center for Teaching & Learning. (2007).
Conference Attendance, "i2 User Conference – Intelligence." (May 2007).
Workshop, "Design & Delivery of Online Instruction," Ferris Center for Teaching & Learning. (May 2007).
Workshop, "Ferris Connect, Overview for Fall Phase-in," Ferris Center for Teaching & Learning. (May 2007).
Seminar, "Visual Analysis training – i2." (May 2006).
Seminar, "EnCase Forensic examiner training." (2005).
Workshop, "Faculty learning community," FSU's Faculty Center for Faculty development. (2005).
Workshop, "Learner-Centered Teaching Workshop," Ferris Center for Teaching & Learning. (2005).
Workshop, "Rethinking College Teaching Workshop," Ferris Center for Teaching & Learning. (2005).
Workshop, "Critical thinking workshop," FSU's Faculty Center for Faculty development.. (2005).
Workshop, "Instructional design workshop," FSU's Faculty Center for Faculty development. (January 2005).

RESEARCH

Published Intellectual Contributions

Refereed Journals

Gogolin, G. & Jones, J. (2010). "*Law Enforcement's Ability to Deal with Digital Crime and the Implications for Business*". *Journal of Digital Forensic Practice*. Taylor & Francis. (forthcoming – republication request received 10/11/10).

Gogolin, G. (2010). "*The Digital Crime Tsunami*". *Digital Investigation*. Elsevier.

Gogolin, G. & Jones, J. (2010). "*Law Enforcement's Ability to Deal with Digital Crime and the Implications for Business*". *Information Security Journal: A Global Perspective*. Taylor & Francis. Volume 19, Issue 3.

Periodicals

Gogolin, G. E. (2009). "*Personal Information Security*". Ludington, MI: The Ludington Daily News.

Gogolin, G. E. (2003). *"The Difference Between Here and There"*. Grand Rapids, MI: The Grand Rapids Press.

Books (contributing author)

Gogolin, G. E. (2011). *Mobile Technology Consumption: Opportunities and Challenges*. IGI Global. (commissioned and in process) – chapter author on the use of embedded mobile, rfid, and augmented reality in mobile devices.

Gogolin, G. E. (2010). *Virtual Worlds and E-Commerce: Technologies and Applications for Building Customer Relationships*. IGI Global. Wrote chapter on security and privacy concerns of virtual worlds.

Other

Gogolin, G. E. (2006). *First Responder Training Curriculum (Digital Crime)- Revised*. Michigan Commission On Law Enforcement.

Gogolin, G. E. (2004). *First Responder Training Curriculum (Digital Crime)*. Michigan Commission On Law Enforcement.

Reviews

Reviewed (2009) forthcoming textbook "Business Intelligence: Practice, Technologies & Mangement," Sabherwal & Becerra-Fernandez, John Wiley & Sons, Inc.

Reviewer for Information Security Journal: A Global Perspective.

Presentations Given

Gogolin, G. E. (Presenter), Secure World, "Digital Crime: Can We Survive the Tsunami?" Detroit, MI. (October 6, 2010).

Gogolin, G. E. (Presenter), Lilly Conference North, "Educating Students and Faculty on the Emerging Use of Virtual Worlds in E-Commerce," Traverse City, MI. (September 25, 2010). (With S. Jones, B.Ciaramitaro, J.Jones)

Gogolin, G. E. (Presenter & Conference Organizer), Ferris State University Digital Forensics Conference for Law Enforcement, "Using Visual Analysis in Computer Crime Cases," Big Rapids, MI. (2010).

Gogolin, G. E. (Presenter & Conference Organizer), Ferris State University Digital Forensics Conference for Law Enforcement, "Cell Phone Digital Forensics," Big Rapids, MI. (2010).

Gogolin, G. E. (Presenter), Lilly Conference North, "Integrating Podcasts, WebEx, Twitter and other interactive technologies into an e-learning environment," Traverse City, MI. (2009).

Gogolin, G.E. (Presenter), Midwest Tribal Security Conference, "Using Visual Analysis and Digital Forensics in Corporate Security," Traverse City, MI. (2009).

Gogolin, G. E. (Presenter & Author), Lilly Conference North, "Using Effective Podcasting to Augment Instruction," Traverse City, MI. (2008).

- Gogolin, G. E. (Presenter & Author), AESA National Conference, "Using Computerized Data to Make Curriculum Decisions," AESA, Savannah, GA. (2005).
- Gogolin, G. E. (Presenter & Author), Banner Oracle Advanced Training. (2004).
- Gogolin, G. E. (Presenter & Author), Banner Oracle Intro Training. (2004).
- Gogolin, G. E. (Presenter & Author), Banner Oracle PL/SQL Training. (2004).
- Gogolin, G. E. (Presenter & Author), Lilly Conference North, "The Effectiveness of Distance Education," Big Rapids, MI. (2004).
- Gogolin, G. E. (Presenter & Author), Oracle 9i Database Administration. (2004).
- Gogolin, G. E. (Presenter & Author), Advanced Microsoft .Net. (2003).
- Gogolin, G. E., Oracle 9i Database Administration, updated. (2003).
- Gogolin, G. E. (Presenter & Author), Web training for teacher and students, Rockford Public School System, Rockford, MI.
- Gogolin, G. E. (Presenter & Author), e-Commerce workshop, Ferris State University, Big Rapids, MI. (2002).
- Gogolin, G. E. (Presenter & Author), Oracle 9i Database Administration. (2002).
- Gogolin, G. E. (Presenter & Author), Oracle 9i SQL. (2002).
- Gogolin, G. E. (Presenter & Author), Database training, Sagestone Corporation. (2001).
- Gogolin, G. E. (Presenter & Author), Fastrack to ColdFusion. (2001).
- Gogolin, G. E. (Presenter & Author), "e-Business," Grand Rapids, MI. (2000).
- Gogolin, G. E. (Presenter & Author), e-Commerce Workshop, Grand Rapids Community College, Grand Rapids, MI. (2000).
- Gogolin, G. E. (Presenter & Author), "Is Your Organization Ready For e-Commerce," ITMA, Grand Rapids, MI. (2000).
- Gogolin, G. E. (Presenter & Author), "e-Commerce in business classes," FSU, Big Rapids, MI. (1999).
- Gogolin, G. E. (Presenter & Author), Information Systems Development Methodology Training, Amway Corporation, Ada, MI. (1999).
- Gogolin, G. E. (Presenter & Author), "Information Systems Project Management," ITMA, Grand Rapids, MI. (1999).
- Gogolin, G. E. (Presenter & Author), Project Management Training, Amway Corporation, Ada, MI. (1999).
-
- Gogolin, G. E. (Presenter & Author), Web training for teacher and students, Amway Corporation, Ada, MI. (1999).

Contracts, Grants and Sponsored Research

Grant

Gogolin, Greg E (Principal), "Acquisition of a Scanning Environmental Electron Microscope," National Science Foundation, US Government, \$871,841.00. (under review).

Gogolin, Greg E (Principal), "Enhance Digital Forensics Capabilities in Information Security & Intelligence and Information Systems Management Programs," Ferris Foundation, Private, \$4,820.00. (2010).

Gogolin, Greg E (Principal), "Software grant/gift in kind – RAM (physical) memory forensics," Sponsored by HBGary, Private, \$64,000.00. (2010).

Gogolin, Greg E (Principal), "Software grant/gift in kind," Sponsored by Choicepoint, Private, \$977,296.00. (2007).

Gogolin, Greg E, "Tech-Literacy Grant," Sponsored by Newaygo County RESA, State Government, \$250,000.00. (2007).

Gogolin, Greg E (Principal), "Software grant/gift in kind," Sponsored by Choicepoint, Private, \$679,780.00. (2006).

Gogolin, Greg E (Principal), "Software/hardware grant," Sponsored by Paraben Corporation, Private, \$9,664.40. (2005).

Gogolin, Greg E (Principal), "Software in kind gift," Sponsored by Quest Software, Private, \$400,000.00. (2004).

Research in Progress

"Digital Forensics Recovery Techniques – Recovering Information from Damaged Media".
Anticipated completion spring 2011.

"Applied research for feasibility and composition of Information Security & Intelligence degree."
(On-Going)

"Capstone Projects" (On-Going)
Extensive research: have directed 150+ capstone projects, the majority of which have a research component.

"Study of effectiveness of distance education (Internet based)." (On-Going)
Extensive: study of effectiveness of distance education (Internet based).

SERVICE

Department Service

Faculty Mentor, Information Systems Management Student Association.
Committee Member, New ISM Student Orientation Committee - Graduate program.
Committee Chair, Program Advisory Board. (2003 - Present).
Committee Member, Faculty Search Committee. (2009).

Committee Chair, Department Tenure Review Committee. (2008 - present).
Committee Member, Faculty Search Committee. (2008).
Committee Member, Faculty Search Committee. (2007).
Committee Chair, Department Tenure Review Committee. (2007).
Committee Chair, Curriculum Development: Information Security and Intelligence. (2006 - 2007).
Committee Chair, Curriculum Development: ISM Curriculum. (2002).
Committee Member, Curriculum Development. (2001).
Committee Member, Faculty Search Committee. (2001).
Committee Member, Graduation Committee - Graduate program. (2001).

College Service

Committee Chair, ISM Academic Program Review. (2010 – 2011).
Committee Chair/Author, New Degree: BS Information Security and Intelligence. (2006 - 2007).
Committee Chair, Core Assessment Team. (2005 - 2007).
Co-chair, Curriculum and Assessment Committee. (2004 - 2006).
Committee Member, Promotion Merit Committee. (2004 - 2006).
Committee Chair, College Curriculum Committee. (2002 - 2006).
Co-Chair, Curriculum and Assessment Committee. (2002 - 2006).
Committee Member, College of Business Strategy Committee. (2003 - 2004).

University Service

Committee Member, University Graduate and Professional Council (2010 – present).
Co-Chair, University Preparedness for Disaster – Technology. (2007).
Consultant. (2006 - 2007).
Committee Member, Banner Steering Committee. (2003 - 2007).
Committee Member, Senate subcommittee on Online Accreditation, Banner Steering Committee. (2003 - 2007).
Committee Member, Banner Oracle License Committee. (2006).
Committee Member, Nursing faculty search/recruitment committee. (2006).
Committee Member, Senate subcommittee on Online Accreditation Standards. (2006).
Committee Member, University Curriculum Committee. (2004).
Committee Member, Banner Oracle License Committee. (2003 - 2004).
Committee Member, ERP Committee. (2003).
Committee Member, Web Advisory Board. (2001 - 2003).
Committee Member, Chief Technology Officer search committee. (2002).
Committee Member, Nursing faculty search committee. (2001).
Committee Member, Nursing faculty search/recruitment committee. (2001).
Committee Member, Web Policy Board. (2000 - 2001).

Professional Service

Reviewer, Grant Proposals, United States Department of Homeland Security (CEDAP). (2006 - Present).

Public Service

Classroom volunteer, Elk Rapids Public Schools, Elk Rapids, MI. (2005 - Present).
Youth Group Leader, Williamsburg United Methodist Church. (2008 – Present).
Workshop Presentation, Newaygo County ISD Employees and Consultants, MI. (2001 - Present).
Event Director, Osceola County Community Foundation - Special Needs Fundraiser, MI. (2003 - 2005).
Board Member, St. Peter's Lutheran Church and School - Board of Christian Education, Rockford, MI.

Classroom volunteer, Rockford Public Schools, Rockford, MI. (1998 - 2004).

Consulting

Boyer USA, Mergers and Acquisitions. (2007 – 2010).

Public and private school systems. (1999 - Present).

For Profit Organization, Rockford Files, LLC. (1999 - Present).

Michigan Commission on Law Enforcement Standards (MCOLES). (2008).

Michigan Commission on Law Enforcement Standards (MCOLES). (2005).

BARBARA L. CIARAMITARO, Ph.D.,
CISSP, CSSLP, PMP

1737 BROADSTONE
GROSSE POINTE WOODS, MI 48236
(CELL) 313 207-6127
E-MAIL (WORK): CIARAMB@FERRIS.EDU
E-MAIL (PERSONAL): BARBARA.L.CIARAMITARO@FRONTIER.COM

EDUCATION

2010 Ferris State University Big Rapids, MI
Currently pursuing a Masters in Business Administration Degree

2007 Nova Southeastern University Fort Lauderdale, FL
Graduate School of Computer and Information Services

- Graduate Certificate in Information Security
- 4.0 Cumulative G.P.A.

2001 to 2005 Nova Southeastern University Fort Lauderdale, FL
Graduate School of Computer and Information Sciences

- Doctor of Philosophy in Information Systems
- Elected to Upsilon Pi Epsilon
- 3.97 Cumulative G.P.A.

1994 to 1996 Central Michigan University Troy, MI

- Master of Science in Software Engineering Administration
- 3.97 Cumulative G.P.A.

1990 to 1993 Oakland County Community College Royal Oak, MI

- Programming and Mathematics Courses
- 4.0 Cumulative G.P.A.

1972 to 1977 Wayne State University Detroit, MI

- Bachelor of Arts with Psychology Major
- Elected to Phi Beta Kappa
- 3.78 Cumulative G.P.A.

PROFESSIONAL CERTIFICATIONS

- Certified Information System Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Project Management Professional (PMP)
- Currently Pursuing Agile Project Management Certification
- Currently Pursuing ISACA Risk Management Certification

ACADEMIC EXPERIENCE

August, 2009 to Present Ferris State University

Big Rapids, MI

Assistant Professor

Information Security & Intelligence

Information Systems Management

Undergraduate & Graduate Courses

- Information Security
- Project Management
- Business Intelligence
- Enterprise Integration
- Risk Management
- Visual Analysis
- Competitive Intelligence Analysis Techniques
- Business Intelligence in Health Care
- Virtual Worlds and Social Media

January, 2011 to Present West Virginia University

Adjunct Professor

- Master in Integrated Marketing
 - Mobile Marketing
 - Digital Marketing Capstone

September, 2011 to Present Norwich University

Adjunct Professor

- Master in Computer Security and Information Assurance
 - Information Assurance Management and Analytics
-

April 2011 to Present Excelsior University

- Developed and taught courses in undergraduate and graduate Cybersecurity Program.

January, 2007 to August, 2009 Walsh College
Troy, MI

Assistant Professor

Business and Information Systems

Undergraduate & Graduate Courses and Topics Discussed

- Project Management
- Information Security
- Social Media
- Internet & Web Technologies
- IT Compliance, Governance and Risk Management
- Software Engineering
- Electronic Commerce
- Current Information Technology Trends and Issues
- Data Warehousing, Modeling and Analytics
- Technology Innovation and Strategy
- Management Information Systems

2007 Nova Southeastern University Online Campus

Adjunct Professor

Graduate School of Computer and Information Sciences

Graduate Courses

- E-Commerce and the Internet

2007 Davenport University Online Campus

Adjunct Professor

Undergraduate Course

- Security Foundations

2005 - 2007

1998 to 2002 University of Phoenix Michigan and Online Campus

Adjunct Professor and Mentor

Information Systems & Technology

Undergraduate & Graduate Courses

- E-Business on the Internet
- Project Management

- Software Engineering
- Database Design
- Information Management
- Networking & Telecommunications

DISSERTATION REVIEW

- 2010 Cappel University
- Participated as an active member of Jerry Solomon's Dissertation Advisory Committee. Dr. Solomon was awarded his Doctorate degree in November 2010.

ACADEMIC MANAGEMENT RESPONSIBILITIES

- April, 2011 to Present Ferris State University
Program Coordinator, Information Security and Intelligence
- Coordinated the building of a strong Program Advisory Board by involving business and academic leaders throughout the state of Michigan.
 - In collaboration with program faculty, assess program distinctiveness and value-added in light of changing stakeholder expectations/needs, adjusting curriculum and programmatic representations accordingly.
 - Utilize social media to increase awareness of ISI program
 - Work with program colleagues to develop internship opportunities for ISI students.
 - Coordinate regular review of program and constituent courses to ensure curricular currency and relevance in light of pedagogical and professional advances, competitive considerations, and changes in workplace needs and expectations.
 - Coordinate assessment activities and assure continuous quality improvement utilizing assessment findings.
 - Coordinate ISI program continuance and expansion at the Main (Big Rapids) and 5 regional campus locations Grand Rapids, Lansing, Midland, Traverse City and Wayne County
 - Coordinate academic advising and recruiting of student at the Main Campus and 5 regional campus locations
 - Recruit and manage adjunct faculty for program.
 - Utilize social media to increase awareness of ISI program
- 2010 Ferris State University
- Program Champion and Advisor to over 30 undergraduate and graduate students in the Ferris Information Security and Intelligence undergraduate program and the Information System Management

graduate program.

PROFESSIONAL DEVELOPMENT

- 2010 Ferris State University Big Rapids, MI
Workshops and Seminars
- Currently organizing a Learning Community on incorporating global competence in undergraduate and graduate education.
 - Quality Matters Online Course Delivery
 - Rubrics and Readability
 - Quality Design Framework for Online Course Delivery
 - Presentation Zen – Improving PowerPoint Presentations
 - Media Chemistry – Incorporating Multimedia into Course Delivery
 - Academic Dishonesty
 - Grant Writing Workshop
 - Data Mining Workshop

PROFESSIONAL EXPERIENCE

- 1999 to 2008 General Motors Detroit, MI
Executive
- Oversight manager for internal and outsourced business processes that provide support for legal and regulatory compliance, information security, information management, electronic discovery, and knowledge management initiatives.
 - Responsibilities include oversight management and decision-making of all security, technology and process components including vendor management, project management, database design and implementation, document management, networking, security and compliance audits, physical and logical access controls, collaborative technologies, and process redesign.
 - Responsibilities include oversight management and decision-making of all operational and contractual issues for outsourced process centers that entail an operational investment of over \$60 million annually.
- 1998 to 1999 Miller Canfield Paddock & Stone Detroit, MI
Director of Information Technology
- Managed the implementation of a new firm-wide (10 office) wide area network that converted from a DOS environment to a distributed client/server Windows NT network. Responsibilities included the oversight of the RFP and vendor selection process, development of appropriate SLAs and service contracts, creation of security and

acceptable use practices, establishment of physical, operational and logical security controls, evaluation and selection of all new office and back-office software.

- Established a Legal Litigation/Practice Support department that provided document and information management services including data collection, database design, document imaging, and document coding through a combination of in-house and outsourced services.
- Provided oversight management for all application development activities including software selection, database design, workflow redesign, and development of Web-based applications.
- Provided oversight management for all network and technology operations including software and hardware monitoring, maintenance and problem resolution.
- Established an in-house training and support team to provide user assistance on utilizing the new technology tools.

1989 to 1998 Plunkett & Cooney

Detroit, MI

Director of Information Systems

- Managed the implementation of a new firm-wide (11 office) wide area network that converted from a mainframe VAX/VMS environment to a distributed client/server Windows NT network. Responsibilities included the oversight of the RFP and vendor selection process, development of appropriate SLAs and service contracts, evaluation and selection of all new office and back-office software.
- Key participant in the design and implementation of a firm-wide total quality management initiative focused on improving work practices to achieve the goal of improved client services, elimination of redundant activities, and greater efficiency.
- Established a Litigation/Practice Support department that provided document and information management services including database design, document imaging, and document coding through a combination of in-house and outsourced services.
- Designed and implemented several firm-wide applications including a case management system, practice development system, and an expert witness system. Also provided oversight management for application development activities including software selection, database design, workflow redesign, and development of Web-based applications.
- Established processes to support IT operations including software and hardware monitoring, maintenance and problem resolution.

PATENTS

2006

General Motors Corporation

Detroit, MI

Inventor

- WO/2005/008528 System and Method for Electronically Managing Discovery Pleading Information
- WO/2005/008380 System and Method for Electronically Managing Privileged and Non-Privileged Documents
- WO/2005/008375 System and Method for Electronically Managing Remote Review of Documents
- WO/2005/008376 System and Method for Electronically Managing Composite Documents

PUBLICATIONS

2011 (In Process) Digital Forensics; Editor: Greg Gogolin, PhD

- Chapter Author
- Chapter Titles
 - *Social Media Forensics*
 - *Social Engineering Forensics*
- Publication Date: Fall 2012

2011(In Process) Security and Privacy in Organizational Cloud Computing: Balancing Risks and Benefits

- Editor and Chapter Author
- Publication Date: Fall 2012

2011 Mobile Technology Consumption: Opportunities and Challenges

- Editor and Author
- Ciaramitaro, B. (Ed). (2011). Mobile Technology Consumption, Opportunities and Challenges. IGI Global. ISBN: 978-1613501504

2010 Virtual Worlds and E-Commerce

- Editor and Author
- Ciaramitaro, B. (2010). Virtual Worlds and E-Commerce: Technologies and Applications for Building Customer Relations. IGI Global, ISBN: 978-1616928087

2008 Secure Software Development – The Role of IT Audit

- Authored by Barbara Ciaramitaro, Oezlem Aras, & Jeffrey Livermore
- ISACA Information Systems Control Journal

1994 *TQM in Action: One Firm's Journey Toward Quality and Excellence*

- Authored by Joseph Walker and Barbara Ciaramitaro
- Details the Total Quality Management initiative at Plunkett & Cooney Law Firm published by the American Bar Association

1993 *Capturing and Leveraging Corporate Knowledge*

- Authored by Barbara Ciaramitaro
- Discusses the benefits of using database technology to manage documents and knowledge published in Paradigm Shift, Vol. 5, No. 2, May 5, 1995

COMMUNITY INVOLVEMENT

- Conducted multiple 6 week workshops for displaced workers on Project Management and achieving Project Management Certification through Walsh College
- Prior Automation Alley Project Lead of Career Awareness Preparation Committee
- Prior Automation Alley Member of Social Media Committee
- Mentor, Michigan Council for Women in Technology

PROFESSIONAL MEMBERSHIPS

- IEEE
- ACM
- PMI
- ISC²
- ISACA
- Association of Virtual Worlds
- Infragard

SEMINARS AND CONFERENCES

August 2011 AMCIS Conference Renaissance Center, Detroit

- Panel presenter on Today's Information Security Challenges
- June 2011 Integrate 2011 West Virginia University
- Current Trends in Mobile Marketing
- July 2011 CISSE Symposium Ohio
- Developing your Digital Persona
- April 2011 PMI Regional Workshop
- Using Social Media in Project Management
- October 2010 SecureWorld Dearborn, MI
- Security and Privacy Issues of Social Media and Virtual Worlds
- September 2010 Lilly Conference Traverse City, MI
- Virtual Worlds and E-Commerce
- 2010 Peace Studies Conference Grand Rapids
- Member of discussion panel on incorporating global competence in the classroom accepted for presentation. (September)
- 2010 Great Teachers Seminar Grand Rapids, MI
- Selected as a faculty member to represent Ferris at the conference.
- 2010 Ferris State University Big Rapids, MI
- Digital Forensic Conference for Law Enforcement*
- Virtual Worlds and Social Media for Law Enforcement
- 2009 URGE Movement Detroit, MI
- Project Management Basics
- 2009 SecureWorld Conference Dearborn, MI
- Employee Privacy
- 2009 Take Charge Workshops Troy, MI
- Project Management Fundamentals

- Preparation for Project Management Professional Certification
- 2008 *SecureWorld Conference* Dearborn, MI
- Secure Software Development
- 2008 *Ideas for Impact Roundtable* Southfield, MI
- Social Media and Privacy Issues
- 2007 *Secure World Conference* Dearborn, MI
- Privacy Challenges in the Global Economy
- 1996 *Sixth International Conference on Software Quality* Ottawa, Canada
- Co-presenter of a tutorial titled *A Training Plan for Introducing TQM into Software Organizations*.

Jerry Emerick, MS, PMP, CISSP VITAE

Rockford, MI 49341
Email: ismjerry@yahoo.com, Phone: 616-951-4676

PROFESSIONAL PROFILE

- Information technology professional with extensive experience in analytical, technical, project management, and educator roles demonstrating a unique versatility and blend of "big picture" and in-depth technical skills.
- Devoted to education, learning, and working with students of all ages and backgrounds to further their knowledge and personal growth.
- I value achieving results, teamwork, helping others succeed, and continuous improvement.
- I enjoy creating solutions to big challenges through teamwork with diverse and talented teammates.

EDUCATION

Master of Science, Grand Valley State University, Grand Rapids, Michigan, 2001

- **Major:** Computer Information Systems
- **Masters Publication** - "Managing XML Data Storage", ACM Crossroads Magazine, Summer 2002
- Additional program certifications obtained in Information Systems Management and Object Oriented Technology

Bachelor of Business Administration, Eastern Michigan University, Ypsilanti, Michigan, 1991

- **Major:** Business Computer Systems

PROFESSIONAL CERTIFICATIONS AND AFFILIATIONS

- Certified Information Systems Security Professional (CISSP) 2011 - Present
- Project Management Professional (PMP) 2004 – Present
- Hyperion Certified Developer and Administrator 2007 – Present
- Microsoft Certified Professional (MCP) 70-229 2005 – Present
- Grand Rapids Community College Curriculum Committee 2004 – 2005
- Certified PowerBuilder Developer 1995 – 1996

TEACHING EXPERIENCE

Instructor Ferris State University 2011 - Present.

Classes Taught – Online and Classroom

- PROJ 320 Project Management – Project management techniques currently employed for business and information systems projects. Course planning projects utilize Microsoft Project software. This course was taught in an online format.
- ISIN 312 - Applications of Information Security - Students apply the tools and concepts of information security in the context of Internet web applications. Students will analyze web

application architecture, tools, and technologies. Students will examine common web application vulnerabilities, how to discover and exploit vulnerabilities, and how to prevent these flaws and vulnerabilities. Students will also apply attack methods for common web application vulnerabilities using ethical hacking and penetration testing techniques.

- HSCJ 202 Principle of Information Security - Students explore the foundations of information security from both historical and emerging perspectives. Topics include critical characteristics of information, attacks, defenses, risk, physical security, disaster recovery, business continuity planning, incident response, cryptography, and malware.
- ISIN 200 All Things Digital - Students investigate various digital devices including computers, cameras, surveillance equipment, and small devices and how to utilize them to advance security objectives. Students also work with various forms of media to understand the capabilities of each. Communication methods and networking are also explored.
- ISYS 470 Advanced Database Administration – Advantages and requirements of client/server computing are discussed. Methodologies for designing, developing, maintaining and disseminating client/server systems are taught. Client/server applications, connectivity issues, software development tools, and database design and implementation methodologies are topics covered. Additional topics include database administration, transaction rollback and commit, data warehousing, data mining, and database security. Projects requiring the design of a distributed data processing network are required.
- MISM 740 Business Intelligence - An investigation of business intelligence and evaluation of analytical data used in strategic decision making. Topics include tracking, managing and understanding organized data, as well as identifying and measuring performance metrics. Includes applied decision making using appropriate tools and techniques. Decision support systems, data warehousing and emerging topics are explored

Adjunct Faculty Ferris State University 2000-2010.

Classes Taught – Online and Classroom

- ISYS 410 Project Management – Project management techniques currently employed for business and information systems projects. Course planning projects utilize Microsoft Project software. This course was taught in an online format.
 - Online / Blackboard Class, Winter 2010
- ISYS 400 - Client Server Implementation - Emphasizes client / server computing, SQL Server database development/administration, and introduces the students to a methodology for developing client/server based applications.
 - Grand Rapids Campus, Fall 2000
 - Grand Rapids Campus, Fall 2003
 - Grand Rapids Campus, Fall 2004
- MMBA 640, Project Management – Guest speaker for various project management topics
 - Big Rapids, Fall 2001

Corporate Training Sessions and Presentations

- IBM Content Manager OnDemand Technical Training
 - 2010, Amway Corporation
- SQL Server Reporting Services Technical Review
 - 2010, Public School Technical and Management Staff
- Microsoft Web Services Development Practices
 - 2009, Amway Information Technology Department
- IBM Content Manager OnDemand Awareness Training
 - 2009, Amway Information Technology Division

- Project Management Training
 - 1999, Amway Corporation
- Advanced Datawindow Techniques
 - 1994, PowerBuilder Developer Users Group, Detroit Michigan 1994

TEACHING INTERESTS

- Information Systems Security
- Database Architecture and Design
- Database Development (SQL)
- Project Management
- Object Oriented Software Design and Development
- Systems Analysis and Design
- Business Intelligence
- Service Oriented Software Architecture

PUBLICATIONS

- **Emerick, Jerry J. (Summer 2002)** "Managing XML Data Storage", ACM Crossroads Magazine

SUMMARY OF WORK EXPERIENCE

Instructor, Ferris State University, 2011-Present.

Senior Software Developer, Alticor Corporation, 2006-Present.

- Lead and participate in information technology projects for the Human Resources division and shared enterprise systems.
- Responsible for all phases of the software development life cycle.
- Utilize industry standard project management processes.
- Promoted after two years of service to Software Advisor.

President, EQS2 LLC, 2005-Present.

- Provide consulting service for software design, development, and search engine optimization.

Project Manager & Technical Team Lead, Gordon Food Service, 2000-2005

- Project Manager, Systems Analyst, and Technical Lead for information technology projects with budgets ranging from \$500,000 to \$1.5 million involving employees, contractors, vendors, and various architectures.

Alticor Corporation, 1996-2000

- **Systems Analyst, Systems Development Architecture Team** - Participated in projects focusing on process improvement initiatives for project management and software life cycle processes. Designer and developer of a suite of Executive Office applications.
- **Senior Programmer Analyst - Warehouse and Inventory Systems** - Developed and enhanced a suite of client/server applications using PowerBuilder, Sybase Adaptive Server Enterprise stored procedures, and Visual C++ that automated many inventory management functions.

Application Developer/Database Analyst, COPPER AND BRASS SALES INC., 1994-1996

- Performed MS SQL Server database administration, systems analysis, design, and development activities. Participated as a team member in the design, development, and deployment of an inside sales system. PowerBuilder and MS SQL Server database technology was utilized for all projects.

Senior Consultant, Ernst & Young, 1992-1994

- Provided information technology consulting services for mid-size to large corporations throughout the Midwest region. Consulting assignments were primarily in the role of a systems analyst or software developer.

CONSULTING

- Business Intelligence – Boyne Inc., 2011 - Present
- Web Site Design and Development –Small Business and Public Education, 2000-Present
- Information Technology Strategic Planning - Election Source, 2006-2008
- Search Engine Optimization –Small Businesses, 2005-2007

COMMUNITY

- President – Rockford Crew Team, 2012 - Present
- Annual Volunteer - Mitchell's Run Through Rockford in support of Duchenne Muscular Dystrophy
- Grand Rapids Community College Curriculum Committee, 2004, 2005
- Class Room Volunteer - Rockford Public Schools
- Head Coach and Assistant Coach - Rockford Little League, 2003, 2004, 2008, 2009

REFERENCES

- Joseph R. Sacco, Sr. Project Manager, Hastings Mutual Insurance, 269-948-1622, joersacco@yahoo.com
- Randy Hoekstra, Cisco Security Professional Services, 616-780-7681, rhoekstr@cisco.com
- Phil Mayrose, Lead Administrator, Alticor Corporation, 616-581-5369, pmayrose@hotmail.com

Adjunct Faculty

Education

M.S. Ferris State University , Big Rapids, MI	2011
Major: <i>Information System Management</i>	
Concentration: Information Security and Network Management	
Capstone Project: Security Awareness: Design and Implementation	
B.S. Davenport University , Grand Rapids, MI	2007
Major: <i>Computer and Information Security</i>	
Supporting area of Emphasis: Network Security	
Capstone Project: Comprehensive Guide to Penetration Testing	
A.A. Grand Rapids Community College , Grand Rapids, MI	2006
Major: <i>Arts</i>	

Certification

• Knock Your Socks Off Customer Service Certificate of Merit – Rockhurst University Continuing Education Center	2012
• Information Security and Network Management – Ferris State University	2011
• ITILv3 Foundation	2011
• CompTIA Security+	2010
• Dell Certified Core Technician	2007
• CompTIA A+	2006

Teaching Experience

• Excelsior College , Albany, NY	2011-Present
Department: College of Business and Technology	
Undergraduate and Graduate Programs	
○ Subject Matter Expert designing and developing course specification, syllabus, lecture content, hands-on activities via cloud environment for the new Cybersecurity program:	
▪ CYS 426 & 526 Cyber Attacks and Defenses	
▪ CYS 475 & CJ 475 Large Scale Cybercrime and Terrorism	
○ Adjunct Professor teaching:	
▪ CYS 426 & 526 Cyber Attacks and Defenses	
• Covering cyber ethics, laws, security	

assessment planning, advanced intelligence gathering, enumeration, vulnerability assessment, exploitation & post exploitation, and assessment reporting

- **CYS 475 & CJ 475 Large Scale Cybercrime and Terrorism**
 - Addressing the emergence of traditional and cyber crime, terrorism, and warfare; the role of technology in facilitating decentralized crime and terrorism; large scale incidents analysis; advanced intelligence gathering; and balancing global scale national security and individual liberties

2011-Present

• **Ferris State University, Big Rapids, MI**

Department: College of Business Graduate Programs

Course: *MISM662 Penetration Testing*

- Subject Matter Expert designed the penetration testing course materials including presentations, assignments, tests, video tutorials, group activities
 - MISM 662 Penetration Testing
- Adjunct Professor teaching the students “A to Z” of penetration testing:
 - Ethics of “hacking” and professional code of conduct
 - Compliance with industry standards and federal, state, local regulations
 - Penetration testing lifecycle: methodology, preparation, planning, execution, post-execution, and reporting
 - Attack-detect-defend hands-on activities via cloud based virtual lab to cover cutting-edge attacking tools and techniques
 - Recommend and implement preventative, defensive, and corrective measures
 - Project management, contingency planning, and risk management

Technical Experience

- **Ferris State University, Grand Rapids, MI** 2007-Present
 - *Technology Services Coordinator* – manage IT projects; a team of two full-time technicians and three student assistants; efforts between IT and contractors/subcontractors; server administration; security policies; network and endpoint security; FERPA, HIPPA, PCI DSS compliance; access control and authentication; data recovery; data encryption; supervise employees; off-campus IT automation and innovation initiatives
- **Grand Rapids Community College, Grand Rapids, MI** 2004–2007
 - *IT Technician* – incident response; system management; workstation security; application scripting and deployment; hardware repair; staff training; part time employee supervision
- **CyberNet, Montana, Bulgaria** 1998–2002
 - *LAN Operator* – system management; malware mitigation; hardware diagnostics; server administration

Publications and Presentations

- “Mobile Technology Consumption: Opportunities and Challenges” published on October, 2011 by IGI Global - chapter co-author with Dr. Ciaramitaro. Exemplified mobile malware risks in order to raise security awareness
- “Introduction to Digital Forensics” by Dr. Gogolin scheduled for publishing on August 15, 2012 by Auerbach Publications. Wrote a chapter revealing and demystifying a wide variety of anti-forensic tools and techniques
- NC-RESA – Presentation - “Web and Social Network Privacy and Security”, 2010
- Ferris State University Technology Newsletters – “Fake antivirus”, “Phishing” articles, 2010
- Digital Forensic Conference for Law Enforcement – Presentation/Demonstration – “Cyber Footprints and Mitigation Techniques”, 2010
- Ferris State Summer University – Presentations – “Online security”, “Malware mitigation”, 2009

Affiliations/Memberships

- Ferris State Technology Standards Committee
- Ferris State Novell Tree Admin Committee
- Ferris State University ITSM Committee

- NAISG - National Information Security Group - Midland, Michigan Chapter
- ITSBA - Information Technology Security Benchmarking Association
- ISSA - Information Systems Security Association - Grand Rapids, Michigan Chapter
- InfraGuard Alliance between the FBI and the private sector - Detroit, Michigan Chapter
- AVIEN - Anti Virus Information Exchange Network
- CompTIA - Computing Technology Industry Association
- SANS - System Administration, Networking, and Security Institute
- Phi Theta Kappa Honor Society – Alpha Upsilon Kappa Chapter – alumni [chapter VP 2005-06]

Interests

- Ethical hacking – methodology, ethics, regulations, tools, techniques, defenses, detection
- Malware – trend analysis, mobile variations, attacking vectors, mitigation, reverse engineering
- Forensics – data recovery, file carving, anti-forensics, privacy & security
- Social engineering and user awareness, training, and education
- Cloud computing – trends, privacy, and security
- Intrusion detection – honeypots, IPS, HIDS, and NIDS
- Contingency planning – incident response, disaster recovery, business continuation and resumption
- Balanced security model – people, processes, and technology

Community Service

- American Cancer Society
- Gilda's Club Grand Rapids
- Susan G. Komen Breast Cancer Foundation
- The Leukemia & Lymphoma Society
- Kid's Food Basket
- Guiding Light Shelter

References available upon request.

Name: James H. (Jim) Jones, Jr.
Address: 10271 Deerpath South, Traverse City, MI 49684
Phone: 231-944-8020 (cell)
Email: jonesjame@saic.com; jonesj54@ferris.edu; jim@secure99.net

EDUCATION

Ph.D. Computational Sciences and Informatics - George Mason University - 2008
M.S. Mathematical Sciences - Clemson University - 1995
B. Industrial and Systems Engineering - Georgia Institute of Technology - 1989

PROFESSIONAL ACTIVITIES

International Association for Intelligence Education (IAFIE): 2008-present
Forum of Incident Response and Security Teams (FIRST): 2000-present
National Incident Coordination Working Group (NICWG): 2001-2003
FedCIRC Senior Advisory Council: 2002-2003
Executive Branch Information Systems Security Committee (EBISS):
 Vulnerability Scanning Tools Issue Group: 2002
National Security Council (NSC) DDoS Task Force: 2001

Certifications: CISSP, Security+, EnCE

RESEARCH INTERESTS

Probabilistic reasoning and machine learning for intelligence and information security problems; compromise and attack detection and defense on computer hosts and networks; digital forensics.

RESEARCH ACTIVITY

Network Topology Discovery (AFRL; 2010-2011).
Botnet Detection (HSARPA; 2006-2009).
National Biosurveillance Integration System (DHS; 2006-2008).
Rootkit Detection and Mitigation (DARPA; 2006-2007).
Detecting Hidden Processes on Compromised Computer Systems (Dissertation; 2006-2008).
Insider Threat Detection (commercial sponsor; 2005).
Active Phishing Detection (SAIC IRAD; 2004-2005).
Automated Digital Forensics (SAIC IRAD; 2003-2005).
SouthWest Border States Anti-Drug Information System (GTRI/DOJ; 1997-1999).
Intelligent Controller (commercial sponsor; 1994-1995).

PROFESSIONAL EXPERIENCE**Assistant/Associate Professor****2007-Present***Ferris State University*

Teach classes in the undergraduate Computer Information Systems (CIS) and Information Security and Intelligence (ISI) programs; teach graduate courses in the Master's of Information Systems Management (MISM) program. Focus is on information security and digital forensics.

Principal Scientist**2002-Present***SAIC*

Serve as Principal Investigator and/or contributing researcher on various R&D projects in the information security and intelligence analysis domain. Previously directed SAIC's Rapid Solutions Laboratory, which conducted quick-turnaround cross-domain applied research to address outstanding problems in the Information Security space. Previously held the positions of Chief Scientist, Operations Chief Scientist, and Group Chief Technology Officer, providing technical content, support, and guidance for multiple information security projects and programs. Responsible for: identifying, evaluating, and matching technical services and products to business unit tactical and strategic needs; identifying, proposing, and leading research and development projects; interfacing with other SAIC business units and programs; and representing the business unit and company at conferences and to customers via papers, briefings, and speaking engagements. Also served as architectural and operational lead for the Federal Computer Incident Response Center (FedCIRC, now US-CERT), as program manager for the Financial Services ISAC, and as technical lead for a strategic acquisition.

Director of Intelligence Operations**1999-2002***SAIC/Global Integrity Corporation/Predictive Systems*

Directed the development and operation of the Analysis Group for SAIC and Predictive Systems' Global Integrity Managed Services, providing collection and analysis of information security vulnerabilities, threats, incidents, and solutions. The Analysis Group operated 24x7x365 and provided the content for various Information Sharing and Analysis Centers (ISACs), delivered the Open Source Intelligence (OSI) service, and served as the Operations Center for FedCIRC. This role included designing and implementing the operational architecture; guiding and participating in technical analysis of security vulnerabilities and threats, including the development of mitigation strategies; preparing detailed analysis on selected information security topics; and data collection and analysis, including the development of new architectures, taxonomies, and models. Previous roles with Global Integrity included: Director of Service Delivery for Monitoring Services, the ISACs, the Incident Response Team, and OSI; Director of the Incident Response Team; and Senior Information Security Analyst conducting computer security incident investigations, providing technical research and analysis on security threats and vulnerabilities, and conducting vulnerability and security assessments. Also directed special research projects, presented and taught at selected conferences, and served on selected committees regarding information security threats and mitigation strategies. Authored a number of articles and technical documents; these and selected comments have been printed in various technical and popular forums; samples are available upon request.

Research Scientist**1997 - 1999***Georgia Tech Research Institute/The Proven Method*

Performed applied research in the areas of computer security and networking, specifically to support the SouthWest Border States Anti-Drug Information System (SWBSADIS).

PROFESSIONAL EXPERIENCE (continued)**Scientist****1995-1997***NISE East / SPAWAR Systems Center Charleston (Department of Defense/Navy)*

Designed architectures and installed computer network security software and hardware (application proxy firewalls, packet filtering routers, and secure network servers) to protect the computer assets of the US Navy. Clearance: TS/SSBI.

Adjunct Faculty**1995***Spartanburg Methodist College*

Taught Introductory Statistics.

Research Assistant and Teaching Assistant**1993-1995***Clemson University*

Developed an intelligent controller for a communications device with funding from a corporate sponsor; designed and coded a simulation of the device in C and devised a control scheme based on an Artificial Neural Network. Taught Introduction to Mathematical Analysis. Taught Computers in the Classroom (computer usage for educators).

HONORS and AWARDS

Letter of Commendation from US Department of Navy for service above and beyond the call: 1997
 Special Recognition from GSA for service to the Federal Computer Incident Response Capability: 2002
 Special Appreciation for a class lecture to State of Maryland IT staff: 2002
 Special Appreciation for a presentation to the American Banker's Association: 2004
 Special Appreciation for a presentation to the Securities Industry Association: 2004

TEACHING EXPERIENCE**Undergraduate**

Digital Forensics and Incident Response
 Advanced Digital Forensics
 Digital Technology and Devices
 Object Oriented Programming
 Discrete Structures
 Introductory Mathematical Analysis
 Introductory Computing
 Introductory Statistics
 Risk Intelligence
 Capstone Experience
 Visual Analysis

Graduate

Systems Integration
 Principles of Information Security
 Advanced Network Security
 Network Penetration Testing
 Network Design and Management
 Advanced Network Design and Mgt
 Integrated Capstone Project

TECHNICAL PAPERS, PUBLICATIONS, and PRESENTATIONS

- *Law Enforcement's Ability to Deal with Digital Crime and the Implications for Business*, Information Security Journal, 2010.
- *Virtual Worlds and the Military*, Book Chapter in "Virtual Worlds and E-commerce", 2010.
- *Detecting Hidden Computer Processes by Deliberate Resource Exhaustion*, GMU PhD Dissertation, 2008.
- *Inducing Observables to Detect Hidden Files and Processes on Computer Systems*, QMDNS, 2007.
- *Automated Computer Forensic Analysis*, DoD Cyber Crime Conference, 2007.
- *Detecting Hidden Files and Processes on Computer Systems*, GMU C4I Annual Review, 2006.
- *Cyberterrorism*, Panelist at Digital Edge Expo, 2005.
- *A Tour of the Phishing Lab*, US Department of Transportation Annual Security Day, 2005.
- *Current Environment - Global Perspective (Phishing)*, FFIEC IT Symposium, 2005.
- *Probabilistic Reasoning for Digital Evidence Analysis*, AAAS Poster Session, 2005.
- *Probabilistic Reasoning for Digital Evidence Analysis*, FIRST Conference TC, 2005.
- *Storm Warnings*, Contributor to Information Security Magazine article, 2004.
- *Incident Response: Techniques, Tools, and Challenges*, Computer Associates Seminar Series, 2004.
- *Application of Bayesian Networks to Digital Forensics*, UAI Workshop, 2004.
- *Successful Application in the Real World: From the Lab to the Field*, UAI Panel, 2004.
- *Phishing Strategies*, presentation to the Securities Industry Association, 2004.
- *Phishing: Keeping Your Customers from Getting Caught*, American Bankers Association, 2004.
- *The State of Information Security*, MRO World Conference, 2004.
- *The Business Case for Secure Information Sharing*, CxO Summit, 2004.
- *Effective Incident Response: Understanding Tomorrow's Threats*, US DoT Annual Security Day, 2004.
- *Intelligence Creation and Information Sharing*, SAIC Internal Document, 2003.
- *New and Emerging Technologies for Information Security*, US DoT Annual Security Day, 2003.
- *BotNets: Explanations and Mitigation*, FedCIRC White Paper, 2002.
- *Incident Response Conference Panel*, Federal Information Assurance Conference, 2002.
- *State Incident Response to Cyber Threats*, Maryland IT Security and Privacy Conference, 2002.
- *Basic Network Security Responsibilities*, US Department of Transportation Annual Security Day, 2002.
- *Energy Sector Takes Aggressive Steps to Enhance Security of Critical Infrastructure*, G&P Journal, 2002.
- *The Internet is a Zoo: Security Trends for 2002*, CIO Magazine, 2002.
- *Security Incidents and Information Sharing*, Seminar series, 2001-2002.
- *Defensive and Mitigation Strategies for the Nimda Worm*, White Paper, co-author, 2001.
- *Luring Hackers to the Honeypot*, Financial Crime Review, 2001
- *Fingers in the Honeypots*, Dallas Business Journal, 2001.
- *Remote Access: Vulnerabilities and Mitigation Strategies*, ISAC White Paper, 2001.
- *Keeping Up With Your Vulnerabilities*, BAI Internet Risk Issues Conference, 2001.
- *SANS Top 20 and AntiVirus Techniques*, Department of Transportation Security Training Series, 2001.
- *The Design and Use of Honeypots*, White Paper, 2001.
- *Enhanced Incident Response through Information Sharing*, FIAC, 2001.
- *Emerging Threats and Defenses*, ComNet Conference, 2001.
- *Information Warfare and Cyber Attacks*, Webcast, co-presenter, 2001.
- *Distributed Denial of Service Attacks: Implications of Recent Trends*, NSC Task Force member, 2001.
- *Mad Hacker: Keeping Your Business Safe from 2001 Security Threats*, Webcast, co-presenter, 2000.
- *Cross-Site Scripting Vulnerabilities*, White Paper, 2000.
- *DDoS Defenses and Mitigation Strategies*, FedCIRC and ISAC White Paper, 2000.
- *Incident Response and Digital Forensics*, 5-day training course, 2000.
- *Advanced Unix Forensics*, IACIS Conference, co-trainer, 2000.
- *The Current and Near Future State of Incident Response*, High Tech Council of Maryland, 2000.
- *The Next Generation of Honeypots*, IACFI Conference, 2000.
- *Distributed Denial of Service Attacks: Defenses*, International Security Forum, 2000.

John K. Herrick
2916 Bluewater LN SW
Grandville, MI 49418
Phone – (616) 893-6907
E-Mail –jherrick@ferris.edu



John Herrick

Teaching Experience:

- **Ferris State University, College of Business, Computer Information Systems –** Adjunct Instructor off and on from September, 1998 until present. Have taught the following classes:
 - ISYS 305 – *Software Systems*
 - ISYS 303 – *Systems Analysis and Design*
 - ISYS 280 – *Advanced Microsoft Word, Excel and PowerPoint*
 - ISYS 204 – *Introduction to Visual Basic.NET*
 - ISYS 105 – *Microsoft Office version 2003, 2007*
 - ISYS 101 - *Introduction to Programming (Visual Basic)*
 - ISIN 190 – *Developing a Web Presence*

- **ITT Technical Institute, Information Technology Department, Grand Rapids Campus, Adjunct Instructor since May of 2001 until present. Have taught the following classes:**
 - BU 131- *Business and Information Systems*
 - PM 331 - *Overview Of Digital Technology*
 - EC 311 - *Introduction to Project Management*
 - EC 324 – *Managing and Maintaining Network*
 - ET 225 - *Network Concepts*
 - IS 318 – *Intranet, Internet and E-Commerce Security*
 - IT 315 – *Web Design Capstone*
 - IT 341 – *Web Security and Ethics*
 - IT 220 – *Network Standards and Protocols*
 - IT 204 – *Web Design*
 - IT 203 - *Database Development (Access, SQL, SQL Server)*
 - TB 143 - *Introduction to the Personal Computer*
 - IT 116 - *Advanced Visual Basic, GUI Design*
 - IT 109 - *Windows XP Professional, Client Side Networking*
 - IT 104 - *Introduction to Programming, Visual Basic and Python*
 - IT 103 - *Operating Systems*

- **Baker College, Information Technology Department, Muskegon Campus, Adjunct Instructor since September, 2005 until present. Have taught the following classes:**
 - INF 111- *Computer Concepts*
 - INF 112 – *Word 2003 , 2007*
 - INF 113 – *Excel 2003, 2007*
 - INF 114 – *Access 2003 and File Management, 2007*
 - INF 121- *Windows XP*

- INF 131- *Internet and WWW*
- INF 141- *PowerPoint 2003, 2007*
- CIS 106 – *Operating Systems A+ Certification*
- CIS 107 – *Computer Hardware A+ Certification*
- NET 101 – *Introduction to Networking Basics*
- **Davenport University**, Lettinga Campus, Grand Rapids, MI. Adjunct Instructor from September 2008 until present.
 - BITS 211- *Microsoft Excel 2007*
 - BITS 212 – *Microsoft Access 2007*

Business Experience:

- **MultiMag, INC.**, 205 S. Higbee St, Reed City, MI 49677. This was an Internet business with over 50,000 sites on the Web. I was the financial officer from 1997 until 2002 part-time. Also designed Web pages.
- **Accounting, tax preparation and bookkeeping for Balanced Tax Service**, 914 Chicago Dr., Jenison, MI. September 1992 through May of 1996. Extensive use of computer, accounting programs (Peachtree, Computer Associate's AccPac, Quick Books) and spreadsheets (Microsoft Excel).

Education:

- **Master of Information Systems Management** degree from Ferris State University. Graduated December 2003 with a Track in E-Business. Have had classes in HTML, ASP, SQL Server Database, PHP, Network Management and Design, Cold Fusion, XML, Project Management, E-Commerce Strategies and more. This degree is both an IT and Management degree.
- **Master of Divinity Degree** from Grand Rapids Baptist Seminary, Grand Rapids, MI. Graduated in May, 1980. Had Administration and Counseling Classes.
- **Bachelor of Science Degree** from Cornerstone University, Grand Rapids, MI. Major in English. Minor in Psychology. Graduated in May, 1977.
- High School Graduate from Allendale High School in Allendale, Michigan. Graduated June, 1972

References:

Dr. James Woolen, Department Head, Computer Information Systems Department, College of Business, Ferris State University, 119 South Street, Big Rapids, MI 49307. (231) 591-2434.

Mr. Eric Hartwell, Department Head, IT Department, ITT Technical Institute, 4020 Sparks Dr. SE, Grand Rapids, MI. 49546 (616) 956-1060.

Dr. Deanna Burt, Dean of Information Technology Department at Baker College of Muskegon, 1903 Marquette Avenue, Muskegon, Michigan 49442, (231) 777-5259.

David J. Auwen

49820 Baker Ct • Macomb, MI 48044

Mobile: 757.277.3593

Email: davidauwen@gmail.com

Education:

- Master of Arts, Diplomacy; concentration in International Conflict Management
Norwich University, Northfield, VT Dec 2008
- Bachelor of Arts, Intelligence Studies; concentration in Terrorism Studies
American Military University, Charlestown, WV Dec 2006

Professional Experience:

HOMELAND SECURITY – CUSTOMS AND BORDER PROTECTION

Feb 2010 – Present

Supervisory Intelligence Analyst – GS-14

- Supervisor of the DHS/CBP Detroit - Intelligence Coordination Team
- Supervise a team of intelligence analysts and task force officers to develop operational and strategic level intelligence products to CBP Field leadership
- Established a Federal Intelligence Working Group to identify similar priority intelligence requirements and create a common intelligence picture
- Provide fused intelligence products to components of CBP
- Produce Operational and Strategic level intelligence products to support CBP missions
- Liaison with national intelligence agencies and local law enforcement in order to answer priority intelligence requirements
- Task Force Officer on FBI Detroit Division - Joint Terrorism Task Force

ADJUNCT PROFESSOR

Aug 2009 – Present

Madonna University – Criminal Justice and Emergency Management (Aug 2009 – Present)

- Teach CJ3500 Homeland Security and Terrorism to University Students
- Teach CJ4110 Ethics in Criminal Justice
- Develop curriculum to achieve course objectives and ensure transfer of learning occurs
- Evaluate students to determine successful completion of university level course

Macomb Community College – Public Service Institute (Aug 2011 – Present)

- Teach HLND1100 Introduction to Homeland Security
- Teach LAWE 1500 Analysis of Terrorism
- Develop curriculum to achieve course objectives and ensure transfer of learning occurs
- Evaluate students to determine successful completion of university level course

DEPARTMENT OF JUSTICE – FEDERAL BUREAU OF INVESTIGATION

Sep 2009 – Feb 2010

Intelligence Analyst – GS-12

- Detroit Division Field Intelligence Groups, Collections Management
- Manage National and Bureau collections requirements
- Identify gaps in intelligence and plan methods to collect against them
- Liaison with national intelligence agencies and local law enforcement in order to answer intelligence requirements
- Write Intelligence Collection Plan for designated division priorities
- Review pertinent intelligence reports and raw data and analyze and assess against requirements

BOOZ ALLEN HAMILTON

Sept 2008 – Sept 2009

Senior Consultant

- Operations Chief for the Associate Director, Ground Systems Survivability, Tank Automotive Research, Development and Engineering Center, Warren, MI
- Update and maintain strategic management system metrics for organization

Continued

- Manage weekly situation reports
- Compile and submit weekly status reports to higher command
- Provide management consulting and make recommendations for management issues

U.S. MARINE CORPS

1997 – Present

Senior Enlisted Leader / Senior Analyst (October 2008 – Present)

Gunnery Sergeant, Joint Intelligence Operations Center, European Command, Joint Reserve Intelligence Support Element, Detroit, MI

- Advise the Director of Joint Operations on all matters pertaining to enlisted issues
- Represent the enlisted troops and perspective during senior level planning processes
- Mentor and train junior Soldiers, Sailors, Airmen and Marines on intelligence and military subjects
- Conduct research and analysis on Military and Political issues on countries within European Commands Area of Operation
- Analyze and Interpret raw data for use in finished intelligence products supporting command

Course Director / Intelligence Instructor (September 2004 – September 2008)

Gunnery Sergeant, Navy Marine Corps Intelligence Training Center, Dam Neck, VA

- Primary block of instruction, Military Operations Other Than War
- Instruct and supervise practical application for link analysis and targeting high value individuals
- Instruct and teach current analytical techniques and methodologies including creative writing, creative thinking, logical fallacies, analytical biases, and analytical tools
- Supervise, train and mentor 14 course team instructors
- Supervise and mentor 150 students through 12 week training program for 18 courses per year
- Update and write curriculum to match current and future intelligence operations requirements
- Conducted Course Curriculum Review Board to identify and develop new course structure
- Master Training Specialist program command coordinator, evaluate and supervise instructors

Infantry Battalion Intelligence Chief (April 2003 – September 2004)

Staff Sergeant, 1st Battalion, 5th Marine Regiment, 1st Marine Division, Camp Pendleton, CA

- Trained and supervised a battalion intelligence shop to be prepared for combat operations in support of Operation Iraqi Freedom (OIF)
- Supervised the Intelligence Preparation of the Battlespace (IPB) process for a Battalion Area of Operations during Support and Stability and Counter-Insurgency Operations
- Tracked over \$300,000 worth of sensitive equipment including computers and camera gear
- Utilized multiple-source reporting to target High Value Individuals
- Managed the battalion collections effort with organic and augmented assets to include; counter-intelligence, signals intelligence, scout snipers and imagery requests
- Supervised the production of intelligence products to support the operations effort of the battalion
- Conducted Sensitive Site Exploitations of targeted houses and facilities in order to gather and exploit intelligence of immediate tactical value
- Utilized crime link in order to produce link analysis products and track terrorist cells
- Gathered and tracked evidence on suspected insurgents for use in legal proceedings
- Supervised IPB on an urban environment for Operation Vigilant Resolve, Al Fallujah

Division Analysis Chief (February 2002 – April 2003)

Sergeant, 1st Marine Division G-2 (Forward), I Marine Expeditionary Force, Camp Pendleton, CA

- During pre-deployment training provided guidance and direction to over 20 intelligence Marines
- Supervised the IPB process prior to combat operations in Iraq
- Wrote a detailed intelligence estimate covering the division area of operations (AO) prior to OIF
- Supervised the production and analysis of intelligence products at the division level during OIF I
- Produced hundreds of products both soft and hard copy for dissemination to subordinate units

Continued

- Utilized C2PC and FalconView in maintaining the common operational picture of a division AO
- Made liaison with higher headquarters and adjacent command to coordinate intelligence effort
- Wrote intelligence reports and daily intelligence summaries for wide dissemination
- Supervised the setup and teardown of the intelligence operations center during combat operations
- Regularly provided intelligence briefs to Division staff officers including general grade officers

Group Intelligence Chief (May 2000 – February 2002)

Sergeant, Marine Wing Support Group – 47, Selfridge ANG Base, Mount Clemens, MI

- Supervised the Intelligence effort for a headquarters and 12 subordinate sites
- Conducted weekly intelligence update briefs to senior officers and staff non-commissioned officers
- As Assistant Security Manager ensured clearances of 300 Marines were updated and validated
- Created monthly training plan for intelligence support to reserve unit
- Served as the unit Colors Sergeant, responsible for numerous color-guards and community events

Intelligence Clerk (May 1998 – May 2000)

Corporal, 1st Battalion, 24th Marine Regiment, 4th Marine Division, Detroit, MI and Special Purpose MAGTF (Experimental), Marine Corps Warfighting Laboratory, Quantico, VA

- As the advanced party intelligence liaison, supervised the setup of the exercise area
- Participated in several Limited Objective Exercises to test future equipment and programs
- Evaluated programs designed to provide common operational picture to the Operations center
- Demonstrated the capabilities of a wearable computer designed for tactical intelligence to the Senate and Congressional staffers in a two day demonstration on Capitol Hill
- Completed designated tasks to support intelligence effort during reserve drill weekends
- Provided current intelligence briefs and produced intelligence products for exercises

Professional Skills and Certifications:

- CBP Supervisor Leadership Training, 2011
- CBP Intelligence Support to Operations Course, 2010
- Federal Bureau of Investigation Academy, Intelligence Basic Course, 2010
- Defense Joint Senior Enlisted Leaders Course, 2010
- Analytical writing for intelligence producers course, 2008
- Master Training Specialist designation, 2006
- Counter-Drug Intelligence Analysis Course, 2006
- Curriculum Developers Course, 2005
- Formal Schools Instructor Course, 2004
- Marine Air-Ground Task Force Intelligence Specialist Journeyman's Course, 2002
- Marine Air-Ground Task Force Intelligence Specialist Entry Level Course, 1998
- Proficient in MS office programs; outlook – power point – excel – word
- Demonstrated excellence in briefing and writing skills
- Proficient in intelligence applications; C2PC, FalconView, Crime-Link, BATS, Analyst Notebook, M3, Automated Case System, TECS, ATS, JWICS

Awards and Achievements:

- Department of Homeland Security Intelligence Leadership Award, 2011
- Navy and Marine Corps Commendation Medal; 2002, 2003 and 2008
- Navy and Marine Corps Achievement Medal; 1999, 2001 and 2004
- Combat Action Ribbon; 2004
- Military Outstanding Volunteer Service Medal; 1999 and 2008
- Navy / Marine Corps Intelligence Training Center Senior Enlisted of 3rd Quarter, 2005
- Selfridge ANG base, Junior Enlisted of the Quarter for the 2nd Quarter in CY 2001
- Eagle Scout, June 1995

Andrew Kenneth Patterson
62884 Crimson Drive
Washington Township, MI 48094
Gov Cell: 586-321-6303
Work: 586-239-3613
Email: andrew.k.patterson@cbp.dhs.gov

United States Border Patrol Detroit Sector Intelligence Unit Selfridge ANGB, MI Supervisory Border Patrol Agent	9/2011 – Present GS 13/2
Selected to be the SBPA for the Detroit Sector Intelligence Unit. Responsible for 13 LBPA's and EAS's. Responsible for planning and executing numerous Intel gathering operations dealing with terrorism, drug smuggling, and human trafficking in the Detroit Sector AOR. As a field supervisor I led Intel teams on surveillance and operations relating to terrorists, gangs and other criminal DTO/HTO's. Liaison with wide variety of local, state, federal (FBI/DEA/ICE/ATF) and international law enforcement agencies (RCMP/CBSA) on various criminal cases. TS/SCI clearance.	
Macomb Community College Warren, MI Adjunct Professor	08/2011 – Present
Asked to develop and teach a border security course for Macomb's Homeland Security concentration program. Course is 16 weeks long, offered fall and spring semester. This is the only course offered like this in the area.	
United States Navy EUCOM Joint Analysis Center Selfridge ANGB, MI HUMINT Target Counter-Terrorism Intelligence Officer	9/2009 – Present Grade Level: O-3
Officer with the United States Navy Reserve, US Forces European Command. Top Secret Clearance required (TS/SCI). Officer in charge of IDX Alpha Team Counter-Terrorism Team. Collect and analyze data pertaining to foreign terrorist targets. Utilize the latest technology, advanced systems, and other agency information (DIA, CIA, NSA, etc) to locate, identify, analyze, and disseminate real-time intelligence target information in accordance with the global war on terrorism in the Middle East. Served as Chief of Joint Intelligence Operations, typically an O-5 position, in charge of 140+ EUCOM joint military intelligence analysts.	
United States Border Patrol Detroit Sector Public Affairs Office Selfridge ANGB, MI Supervisory Border Patrol Agent	8/2009 – 9/2011 GS 13/1
Selected to head-up the Detroit Sector Public Affairs Office representing the Detroit Sector Border Patrol. Duties include spokesperson for the sector, coordinating/handling media events, issue press releases to local, national, and international news agencies, coordinate VIP visits, congressional affairs liaison, and community outreach liaison.	
United States Navy Defense Intelligence Agency Rome, NY Target Imagery Intelligence Officer	10/2008 – 9/2009 Grade Level: O-3
Officer with the United States Navy Reserve, Defense Intelligence Agency (DIA). Top Secret Clearance required (TS/SCI). Collect, analyze, and brief imagery data on specific target locations within specific countries throughout the Middle East.	
United States Border Patrol Swanton Sector / Ogdensburg Station Ogdensburg, NY Border Patrol Agent	6/2008 – 8/2009 GS 11/2
Accepted a VRP to Ogdensburg Station as a field agent. Volunteered for midnight shift during my time there. Worked with Sector Intel on illegal drug smuggling in the Ogdensburg AOR. Created relationships with local hotels/motels in order to gain cooperation in alerting us to suspicious activity and suspicious persons checking-in at their establishments. This effort resulted in numerous apprehensions and illegal drug-smuggling arrests to include a large drug smuggling ring in New York State.	

**United States Navy
COMPACFLT
Intelligence Officer**

**1/2006 – 9/2008
Grade Level: O-1 – O-2**

Officer with the United States Navy Reserve, Commander Pacific Fleet. Top Secret Clearance required (TS/SCI). Collect and analyze strengths, weaknesses, capabilities, and intentions of US military interests abroad as it relates to the USS Ronald Reagan and USS Abraham Lincoln Carrier Strike Groups.

**United States Border Patrol
Yuma Sector / Yuma Station
Border Patrol Agent**

**8/2005 – 6/2008
GS 5/1 - 11/1**

Assigned to the USBP's Yuma, Arizona Station. Worked as a field agent during the time period when Yuma was apprehending over 800 bodies per day and seizing hundreds of pounds of illegal narcotics nightly. Detailed to the Yuma Station Disrupt Team (anti-smuggling unit). Assigned to "high traffic areas" usually in remote locations throughout the Yuma Station Area of Operations (AOR).

**KCMS
Chittenango, NY**

8/2004 – 7/2005

Vice President, Sales & Marketing

Responsible for all corporate sales/marketing efforts, and staff for an IT consulting company servicing the financial services, environmental, and medical industries. Responsible for network design, development of LAN's & WAN's, PC & sever requirements, software requirements, and technical integration of various software products. Technical knowledge of Windows based products, and various industry specific 3rd party products (platforms varied). Managed all corporate sales, marketing/advertising, and partnership/alliance initiatives strategies and personnel. In charge of corporate growth and establishing business networks with potential partners and customers. Oversee market penetration, trade shows, and official meetings. Manage revenue, cost savings, and corporate initiatives.

**ProAct Pharmacy Services
Syracuse, NY**

10/2003 – 2/2004

Regional Business Manager

Manage northeast regional territory for pharmacy benefits management company. Responsible for 50% sales and 50% business/market penetration and growth. Managed existing client relationships and advised various organizations on prescription drug benefit plans as well as analysis on drug costs vs. revenue savings. Managed all corporate marketing/advertising and partnership/alliance initiatives strategies and personnel. Hired to grow the organization from a small northern NY company to a Northeast Regional PBM. Left company after accepting a position closer to my geographic area.

**PCi Corporation
Boston, MA**

9/2002 – 8/2003

Senior Project Manager

Managed project teams, processes, procedures, resources and activities relating to client software implementations for the US Banking Industry. Responsible for pre-implementation technical readiness, network consultation, IT requirements, software integration, and software testing. Created project plans, technical scoping documents, and corporate technical product documents. Managed client expectations/correspondence, beta programs, and performed analysis on client's technical infrastructure. Responsible for multiple internal and external departments throughout project life cycle. Manage relationships with client throughout implementation and deployment process. Left company to relocate to Syracuse, NY for my wife's job.

**Firepond Inc
Waltham, MA**

11/2000 – 10/2001

Senior Technical Business Consultant

Evaluated viability of new clients during pre-sales process. Presented recommendations to CEO. Authored / evaluated responses to all RFP/RFI's. Developed & Presented sales presentations and product demonstrations. Cultivated relationships with potential clients upper level executives and performed analysis on their business goals, plans, and procedures. Utilized consultative sales methodologies and developed personalized proposals to meet significant business solutions. Managed corporate competitive positioning and responsible for sales reps on all company products and services. Selected by the CEO and VP of Public Relations to deliver corporate presentations to US industry analysts.

Lightbridge Inc
Burlington, MA

2/1997 – 10/2000

Senior Sales Consultant

Evaluated and assessed new and existing clients reporting findings directly to the VP of Sales. Interacted with client's upper level executives to understand business goals, plans, and procedures. Managed corporate competitive positioning and stayed educated on all company products & services. Authored responses to all Requests for Proposals/Requests for Information. Developed & presented client presentations and product presentations. Technical knowledge of product offerings based in UNIX and Windows was necessary. Advanced technical knowledge of all company products as well as technical integration of those products was also necessary. Left company after accepting another position

Senior Account Manager

Promoted to lead account/sales team for the largest revenue account, AT&T Wireless. Responsible for sales and relationship management for AT&T Wireless USA. In one year I turned the account around from a poor level to the most satisfied client. Evaluated and assessed new & existing AT&T projects, procedures, and sales opportunities. Met with AT&T's upper level executives to evaluate their business goals, plans, and procedures. Managed all AT&T product deployments, and new market roll outs. Promoted to Sales Consultant.

Project Manager

Managed project teams of up to 30 people. Projects ranged from localized projects costing \$5 thousand to national initiative projects costing over \$8 million. Products were UNIX & Windows based platforms. Technical knowledge of both platforms was necessary. Was only employee asked by client to work 8 months on-site at AT&T HQ in Redmond, WA. Planned and coordinated all resources and managed project development & implementations for all system modifications. Promoted to National Account Manager.

Technical Support Manager

Developed programs to ensure high levels of customer satisfaction for entire customer base. Hired, trained, and developed a team of twenty-five technical support representatives. Job required technical knowledge of UNIX based software products and Windows based software products. Promoted to Project Manager.

Merisel Inc

Cary, NC

Account Executive

Responsible for distribution sales to Eastern US VAR Channel of computer hardware and software representing over 200 manufacturers.

EDUCATION

F.W. Olin Graduate School of Business at Babson College

5/2003

Babson Park, MA

Masters Degree in Business Administration (MBA)

60 Semester hours

Concentration in International Business and Entrepreneurship

LeMoyne College

5/1995

Syracuse, NY

Bachelor of Science in Business Administration

120 Semester hours

Concentration in Business Administration & Marketing

REFERENCES

Lloyd Easterling Assistant Chief Patrol Agent	United States Border Patrol Lloyd.m.easterling@cbp.dhs.gov	Tucson Sector 586-239-3613
Matt Donaldson Assistant Chief Patrol Agent	United States Border Patrol matthew.h.donaldson@cbp.dhs.gov	Detroit Sector 586-239-2167
Carlos Aguilar Assistant Chief Patrol Agent	United States Border Patrol carlos.i.aguilar@cbp.dhs.gov	Detroit Sector 586-239-2168
Glenn Lendel Patrol Agent in Charge	United States Border Patrol glenn.m.lendel@cbp.dhs.gov	Miami Sector 813-623-5101

JOB RELATED TRAINING/SCHOOLS

2012 U.S. DEA Confidential Informant Handling Course
2011 Michigan State Police Surveillance School
2011 Counter-Drug Intelligence School
2011 Military Operational Security Training (OPSEC)
2011 U.S. CBP Detecting Deception and Eliciting Response Training
2011 U.S. CBP Incident Command Systems 300 Training
2010 MCOLES Interview & Interrogation Training
2010 Bureau of Justice Anti-Terrorism Training
2010 U.S. CBP Supervisor Leadership Training (SLT)
2010 U.S. Border Patrol Supervisor Training (TTC)
2010 U.S. CBP Situational Leadership Training
2010 U.S. CBP Leadership Skills for Addressing & Preventing Corruption
2009 U.S. CBP Public Affairs Training
2009 U.S. CBP Creative Problem Solving
2007 FBI JTTF Islamic Extremist Training
2007 U.S. Border Patrol Recruiter Training
2007 Advanced Military Intelligence School
2006 Basic Military Intelligence School
2005 U.S. Border Patrol Basic Academy, Class 597

AWARDS

2012 - Joint Meritorious Unit Commendation
2011 - United States Border Patrol Monetary Award
2011 - Military Outstanding Volunteer Service Medal
2010 - Information / Intelligence Dominance Warfare Qualification
2010 - United States Border Patrol Monetary Award
2009 - Meritorious Unit Commendation
2008 - United States Border Patrol Non-traditional Award
2007 - United States Border Patrol Monetary Award
2007 - Global War on Terrorism Medal
2007 - United States Border Patrol Non-traditional Award
2006 - Expert Rifle Medal
2006 - Expert Pistol Medal
2005 - National Defense Medal

SUMMARY:

Proven Information Security professional with extensive experience with vulnerability assessments, penetration testing, firewalls, intrusion detection and prevention systems, risk assessment/risk management, audit and compliance, IT governance and security policy development and implementation.

EDUCATION:

Fort Hays State University

- Master of Liberal Studies – Information Security Management

Online

2012

Davenport University

- Bachelor of Applied Science – Information Assurance

Midland, MI

April 2009

CERTIFICATIONS – Current:

- Certified Information Systems Security Professional
- Certified Information Security Manager
- Certified Ethical Hacker
- Computer Hacking Forensic Investigator
- CompTIA Security+; CompTIA Network+; CompTIA A+
- Microsoft Certified Systems Administrator; Microsoft Certified Systems Engineer
- SANS GIAC Certified Forensic Examiner

CERTIFICATIONS – Past:

- Cisco Certified Network Associate; Cisco Information Security Specialist
- Compaq Accredited Systems Engineer; Compaq Accredited Systems Integrator
- Novell Certified Network Administrator

EXPERIENCE:

Chemical Bank

January 2012-Present

Manager Security Operations & Architecture

- Develop, maintain and implement processes for detecting, identifying, and analyzing information security incidents.
- Coordinate and manage periodic testing of incident response plans
- Manage technical investigations and artifacts analysis of network penetration attempts, computer intrusions, security anomalies, and attacks against the information security infrastructure
- Review, collaborate, and develop security documentation; provide project management and leadership for security related projects.
- Manage the day-to-day information security operations and personnel.
- Oversee incident response planning as well as the investigation of security breaches, and assist with disciplinary and legal matters associated with such breaches as necessary.
- Monitor logs/reports from servers, mainframe, firewalls, intrusion detection, network traffic, Email, Internet usage, and access administration for unusual or suspicious activity/violations. Interpret activity, recommend plans for resolution.

- Implementation and administration of Security Information and Event Management (SIEM) solution.
- Monitor system compliance with corporate security standards.
- Assist and participate in technology based audits and risk assessments.
- Monitor industry trends and best practices relating to our products and environment and recommend additional security products and tools, or enhancements to existing tools to detect violations of network security measures.
- Monitor integrity and confidentiality of information residing in corporate databases, workstations, servers and other systems.
- Assess and communicate all security risks associated with implementations to CIO.
- Provide expertise and assistance performing Risk Assessments.
- Monitor public information sources for newly published security vulnerabilities.

Chemical Bank

March 2008-January 2012

Information Security Specialist

- Create and implement information security standards and policies in accordance to COBIT and ISO 27001/27002 framework.
- Monitor logs/reports from servers, mainframe, firewalls, intrusion detection, network traffic, Email, Internet usage, and access administration for unusual or suspicious activity/violations. Interpret activity, recommend plans for resolution.
- Implementation and administration of Security Information and Event Management (SIEM) solution.
- Promote implementation of various security initiatives, including Information Security Awareness Program that included an online learning system (LMS).
- Monitor system compliance with corporate security standards.
- Ensure that users understand and adhere to necessary procedures to maintain security.
- Assist and participate in technology based audits and risk assessments.
- Monitor industry trends and best practices relating to our products and environment and recommend additional security products and tools, or enhancements to existing tools to detect violations of network security measures.
- Monitor integrity and confidentiality of information residing in corporate databases, workstations, servers and other systems.
- Assess and communicate all security risks associated with implementations to CIO.
- Provide expertise and assistance performing Risk Assessments.
- Monitor public information sources for newly published security vulnerabilities.
- Perform audit reviews of security logs and user permissions through system generated and manual reports.
- Document processes and procedures related to tasks performed.
- Conduct forensic analysis of computer evidence and provide continuing technical support involving hardware, forensic analysis tools, and computer files, including recommending file review and search procedures based on knowledge gained during seizure and recovery.
- Performed due diligence for key vendors in accordance with Vendor Relations Program, On site review of physical as well as logical controls, and SAS70 reviews.

AHIS-St. Mary's of Michigan

January 2007-March 2008

Information Security Officer

- Developed and delivered IT security policies, standards, guidelines and best practices in accordance with COBIT and ISO 27001/27002 to ensure information security across the enterprise.
- Implemented processes and methods for auditing and addressing non-compliance to information security policies and standards.

- Assisted in security investigations and provided data/information for internal investigations from an information systems perspective.
- Directed and implemented necessary controls and procedures to cost-effectively protect information systems assets from intentional or inadvertent modification, disclosure, or destruction.
- Participated in IT security assessments, audits, and examinations.
- Managed and mentored the organization's information systems incident response team, which handles network intrusions, security breaches, cyber attacks, and internal investigations. Led the local Incident Response Team.
- Conducted risk and security assessments and enterprise security management tool evaluations.
- Provided direction for HIPAA Security and IT Security user training and development programs.
- Reviewed and scrutinized proposals for security design considerations.
- Identified and developed solutions for potential security exposures on systems.
- Collaborated with Disaster Recovery Coordinator and other IT management, to review overall D/R plan for the entire health system with regards to Business Impact Analyses, site recovery contracts, system testing and review of system vulnerabilities.
- Provided regular status reports to CIO and Director on outstanding department security issues.

Analysts International

October 2006-December 2006

Senior Security Consultant

- Responsible for Cisco host based IDS deployment for educational system with over 6,300 students
- Led project for global manufacturing company to re-mediate SOX audit findings including implementation of a log management system.
- Protected internal data systems with anti-virus software, intrusion prevention, border security devices and wireless security.
- Analyzed firewall configuration and traffic.
- Connected remote offices securely.
- Safeguarded externally accessible hosts like the Web, mail, and database servers.
- Used investigative forensics to recover from a security incident.

The Rehmann Group

November 2005-October 2006

Senior Information Risk Specialist

- IT Security Audits – Hands on review of Servers, Firewalls, Routers, and other network infrastructure devices to meet best practice standards.
- Responsible for creating audit guidelines for Windows, Linux, and iSeries systems.
- IT SOX consulting – Acted as Internal/External Auditor for SOX 404 audits.
- GLBA consulting – Created policies for clients, including Information Security Program, Incident Response Program, and Acceptable Use Policies.
- Conducted Penetration Testing/Vulnerability Assessments.
- Setup and administered in house Managed Vulnerability Service for clients.
- Created all courseware/labs and instructed a Network Security Clinic for clients that included best practices for securing Cisco Routers and Firewalls.
- Conduct forensic analysis of computer evidence and provide continuing technical support involving hardware, forensic analysis tools, and computer files, including recommending file review and search procedures based on knowledge gained during seizure and recovery.

Community Mental Health for Central Michigan

October 2002-November 2005

Network Administrator/Information Security Officer

- Network/System Administrator for 500 user, 9 site WAN/LAN environment.
- Installed, maintained and supported Domain Controllers, File Servers, Mail Servers and Citrix Servers.

- Maintained backups and file restorations.
- Installed, maintained and supported Firewall/IPS; Cisco routers and managed switches; CAT5 cable; SNORT based IDS
- Oversaw network security and penetration testing of internal networks.
- Performed Risk Assessments.
- Created, implemented, and enforced security policies; HIPAA security and guidelines
- Used protocol analyzer to troubleshoot network performance.
- Conducted end user training.

Solutions Plus, Inc.

May 1999-October 2002

Systems/Network Engineer

- Maintaining LAN, servers and workstations at our location.
- Installed and configured servers and workstations on site for clients; hubs, routers, and switches; CAT5 cable; Compaq, HP and IBM servers.
- Completed warranty repair and diagnostic testing on servers and workstations.
- Trained technicians and sales staff in basic network concepts.
- Served as system administrator in-house and for clients and managed PC technicians and network engineers.

Advanced MicroElectronics, Dow Chemical Company

January 1997- May 1999

Desktop Support Specialist

- Maintained workstations in an NT environment.
- Performed Hardware and Software break/fix support.
- Trained users on various software applications.

Dow Chemical

February 1996- January 1997

Computer Technician

- Assisted in implementation of workstation roll-out.
- Set up PC's, installed hardware and software upgrades and supplied basic network troubleshooting.

PROFESSIONAL ASSOCIATIONS:

- Chairperson - Midland, MI Chapter of the National Information Security Group (NAISG)
- High Technology Crime Investigation Association (HTCIA)
- Information Systems Audit and Control Association (ISACA)
- Business Espionage Controls & Countermeasures Association (BECCA)
- InfraGard - Detroit, MI Chapter

CHRISTOPHER JAMES CONGER

(MILITARY VETERAN)

316 N Harrison, Ludington
Michigan, 49431
christopher.conger@gmail.com
congerc@ferris.edu
(989) 928-5245 CELL

OBJECTIVE

Seeking an entry level position as adjunct professor with Ferris State University teaching Information Security and Intelligence.

HIGHLIGHTS OF QUALIFICATIONS

- Government Secret Security Clearance
- Chaired the 911 "Honoring American Heroes" event at Ferris State University.
- Scored in the top 1% percent of Air Force on E-5 (SSgt) test.
- Awarded Distinguished Graduate from USAF Air Education and Training Command
- Able to make difficult decisions in stressful situations

EDUCATION

Information Systems Management, Master of Science

Ferris State University, Big Rapids, Michigan
August 2010 – May 2012
GPA 3.44/4.0

The MS-ISM program focuses on the concepts and skills for effective leadership and includes concentration choices in emerging areas such as outsourcing management and several technical areas with growing career potential.

Information Security and Intelligence, Bachelor of Science

Ferris State University, Big Rapids, Michigan
August 2008 – December 2010
GPA 3.83/4.0

Studies focused in a variety of leading edge technologies such as link/visual analysis, geographic information systems, and digital forensics, as well as a broad cultural background to provide a basis for interpreting information and its ethical use.

Security Forces Apprentice Course, Certification

Community College of the Air Force, Lackland AFB, Texas
January 2003 – April 2003

343rd Training Squadron focuses on teaching missile security, convoy actions, capture and recovery of nuclear weapons, law enforcement, directing traffic and nonlethal tactics such as using pepper spray and pressure points on a body.

Criminal Justice, Bachelor of Science

Northern Michigan University, Marquette, Michigan
August 1998 – May 2002
GPA 2.9 /4.0

Studies focused on the basic understanding of the criminal justice system and its components. Specialized courses included community policing, law enforcement function, criminology, and investigative process.

Skills

Adobe Photoshop CS4
Digital Forensics
GIMP
i2 Analyst's Notebook
Linux
MS Excel
MS Access
MS Surface
SLES 10
Visual Basic 2005
VMware
Web
MS SQL
Oracle

Licenses

Michigan CCW

EXPERIENCE

Teaching Assistant

August 2010 – Present

Newaygo County Regional Education Service Agency - Ferris State University
Farmington, Michigan

Assisted Ferris State University Faculty in teaching various aspects of the use of virtual worlds and social media by various domains including a discussion of the elements of virtual worlds, current examples of virtual worlds in use by various businesses and other organizations, the potential economic gains of utilizing virtual worlds, legal, security, privacy and technological issues, human factor issues in virtual worlds, and the future of virtual worlds and social media. Demonstrated several different social media tools used for personal and business purposes. Provided lectures and discussions pertaining to social media on a regular basis.

VA Work Study Assistant

August 2009 – August 2010

Ferris State University
Big Rapids, Michigan

Assist veterans by explaining education benefits according to Department of Veterans Affairs Policy and current laws. Provided accurate and timely information regarding benefits entitled to each veteran when questioned. Confirmed veteran enrollment status and prepared certification through VA-Once. Directed veterans to specialized help when requested. Assisted veterans in filling out documents for benefits. Established a new filing system for veteran's paperwork. Designed certificate for individuals who participated in veteran events around campus. Helped design banners for the Supportive Education for Returning Veterans Room (SERV) located on campus.

Machine Operator/General Laborer

September 2007 – August 2009

Chase/Arbre Farms
Walkerville, Michigan

Supervised a group of 20 or more people for two weeks on second shift in the packaging department. Operated a poly bag machine designed to package various types of fruits and vegetables. Provided maintenance and operation of the plant's one million dollar Bertocchi turbo extractor machine used to produce puree. Operated a forklift during high periods of production. Responsible for cleaning work area and all associated machines or equipment.

Security Forces Member

December 2002 – December 2006

49th Security Forces Squadron
Holloman AFB, New Mexico

Provided protection for over 17,000 personnel, 59,000 acres, 1,280 housing units, and 945 dormitory rooms. Provided traffic control and enforcement while assisting motorists with instructions and directions. Enforced New Mexico state traffic laws and Air Force Regulations. Issued citations and apprehended personnel in violation of state laws and the Uniform Code of Military Justice. Responded and investigated traffic accidents; administered first aid when necessary. Established and preserved crime scenes, conducted criminal investigations, collected and protected evidence for court. Provided immediate armed response to security incidents, hostile situations and alarm activations overseas and in the United States. Ensured the protection for Protection Level (PL) 2 Space Surveillance assets, PL 3 aircraft and other resources requiring stringent security measures. Deployed to Balad Air Base, Iraq in support of Operation Iraqi Freedom. Conducted off-base patrols; dominated key terrain surrounding the base, and reduced indirect fire. Scored an outstanding 92% on Security Forces Apprentice End of Course test; unharmed in a combat zone. Certified Advantor and Intrusion Detection System alarm monitor; Monitored alarms and dispatched patrols accordingly

ACTIVITIES, AWARDS, & ADDITIONAL TRAINING

Treasurer, Ferris State University Veterans Association, 2010
National Honor Society, 2009
Upper Division Academic Scholarship, 2009
Ferris State University Veterans Scholarship, 2009-2010
Ferris State University Veterans Scholarship, 2008-2009
Dean's List of the College of Business, Ferris State University, Fall 2009
Dean's List of the College of Business, Ferris State University, Summer 2008
Dean's List of the College of Business, Ferris State University, Spring 2009
Dean's List of the College of Business, Ferris State University, Fall 2008
Volunteer, Walkerville Public Schools, 2009
Promotion to Staff Sergeant, 2006
AF - DOD Combating Trafficking in Persons Certificate, 2006
Nuclear, Biological, Chemical Defense Training (NBCDT) Certification, 2005
Law of Armed Conflict, Anti-Terrorism, and Code of Conduct Briefing, 2005
Self-Aid Buddy Care, 2005
Letter of Appreciation from 332ND Expeditionary Security Forces Commander, 2005
Dead Eye Award from NCOIC Combat Arms, 2005
332nd Expeditionary Security Forces Airman of the Month, 2005
332nd Expeditionary Security Forces Certificate of Recognition for 92% EOC Exam, 2005
Volunteer, Bataan Memorial Death March, 2005
Promotion to Senior Airman, April 10, 2005
AFCESA - Explosive Ordnance Reconnaissance Course, 2005
Communication Procedures, 2005
Cope Training, 2005
PR/AED, 2005
Defensive Fighting Positions, 2005
Patrolling, 2005
Retrograde Operations, 2005
Handcuffing, 2005
Secure Crime Scene, 2005
Suicide Prevention/ Violence Awareness, 2005
Use of Force, Concepts and Principles, 2005
Victim, Witness, Assistance Program, 2005
Letter of Appreciation from 49th Security Forces Commander, 2004
Letter of Appreciation from 49th Security Forces First Sergeant, 2004
Distinguished Graduate for the Security Forces Apprentice Course, Class 030204, 2003
Wing Chun Kung Fu - Assistant Instructor Certification 2000
Air Force Training Ribbon
Air Force Overseas Ribbon Short
Global War on Terrorism Service Medal
Global War on Terrorism Expeditionary Medal
Iraq Campaign Medal
Armed Forces Expeditionary Medal
National Defense Medal
Air Force Good Conduct Medal
Air Force Outstanding Unit Award
Meritorious Unit Award

Appendix C: Course Syllabi



Ferris State University

College of Business

COURSE: ISIN 200 All Things Digital (82458)

Instructor: Jerry Emerick, MS, PMP, CISSP

Phone: (616) 951-4676 (mobile / preferred) or (231) 591-3148.

Email Address: Ferris Connect (Preferred) or ismjerry@yahoo.com

Online Instruction: Ferris Connect / Learn (the new Ferris Connect)

Classroom: BUS 121, Thursday, 6 PM to 8:50 PM

Course Dates: August 29th to October 18th, 2011

Office Hours: 1:30 to 5:30 p.m. Thursday in Big Rapids; Other times available by appointment.

Communication – Please use Ferris Connect as your primary method of email and for submitting all assignments. I will make every attempt to return all email and phone calls within 24 hours. However, in the event you have not received a response within 24 hours please do not hesitate to reach out to me again. Many assignments are due on Sunday no later than 11:59 PM. It is strongly encouraged to not wait until the weekend to contact me for assistance as there are times when I will be less available on the weekends. Email may be more effective on the weekends when necessary. I encourage office hour visits. Please don't hesitate to stop by.

Course Description

You will learn basic through advanced computer concepts with an emphasis on digital devices, personal computers, enterprise computing, and information security. Topics include hardware, application and system software, the Internet, communications, database management, software design, programming, career opportunities in the computer field, and computer trends. Many course topics will emphasize information security.

Through interactive lectures, classroom labs and assignments you will:

- Become proficient with using virtual machines such as VMWare.
- Learn and utilize DOS and Linux operating systems commands.
- Learn the basics of binary and hex and become comfortable analyzing various file types such as images using a hex editor.
- Become familiar with various aspects of information systems security.
- Be introduced to networking fundamentals
- Use communication tools such as FTP
- Create a basic relational database, load, query data, and analyze physical file structures.
- Understand and apply web application architecture
- Become familiar with potential careers and professional certifications

Course Format

This course will be conducted as a "double pace", 7 week course. We will meet once a week in class and throughout the week in Ferris Connect for the online / web delivery portion of the class. The class will primarily consist of interactive lectures, individual assignments, and group exercises.

Course Materials



Title: Discovering Computers 2011: Complete
Author: Shelly Cashman
Publisher: Course Technology; 1 edition
ISBN-10: 1439079269

Policies

Attendance and Participation - Attending class regularly and actively participating is the best way to succeed in this class. Research has shown that student attendance and participation is critical. In order to support your ability to succeed I have made attendance and participation a factor in your final grade. This should be the easiest outcome to achieve in this class. Successfully participating in class includes arriving on time, staying until the class is dismissed, not being disruptive, no excessive use of mobile phones and laptops for purposes other than taking notes, actively participating in group activities, and **posting to Ferris Connect discussion topics.**

Assignments - **All classroom assignments are due no later than Sunday by 11:59 PM unless otherwise stated. All online assignments are due no later than Wednesday by 11:59 PM unless otherwise stated. ALL assignments are to be submitted via Ferris Connect.**

Make-up Policy - There will be no make up quizzes, exams, assignments or discussion question postings. It may be possible to pre-schedule a quiz or exam but students must contact the instructor directly and this will be determined on an individual basis.

Syllabus Changes - Adjustments to the syllabus may be necessary when it is determined that the adjustment(s) will better serve the overall learning needs of the class. We will discuss these changes together in class.

Discussions – Ferris Connect - Discussion topics may be posted on Ferris Connect during this course. Students will be required to participate and interact with one another during the semester on the course discussion boards. You are required to create at least one original reply to the instructor's discussion topic and respond to at least two of your classmates for each discussion question posted. Early posting in the

Discussion will ensure you receive replies from fellow students. Your discussion posting will be graded using the following grading rubric.

Discussion Questions Grading Rubric

Points	Description
10 points	Responded to all questions with interaction among other students. Responses began early and were often. Responses were thoughtful and topical. Outside sources, previous knowledge, and real life experience were used in responses. The flow and direction of the discussion was greatly affected by contribution.
6 to 9 points	Did not respond directly to all questions, and/or did not respond to others with comments or questions and/or all responses are made in one visit to the site. Responses lacked deep analysis or thought..
5 or less points	Minimal participation. Did not respond to all posted questions. All responses are made in one visit to the site. Responses lacked analysis or thoughtfulness (applied text or lecture teaching points or real life examples) and/or was not topical (related to the text and lectures.)
0	No participation. No response

Course Points and Grading Scale

Course Points

Grading Scale

Your performance will be assessed as follows:

Your grade will be calculated as follows:

Assessment	Total Points
Class Labs (7 @ 20 points)	140
Assignments (10 to 30 points)	200
Quizzes (3 @ 30 points)	90
Final	100
Participation / Attendance	70
Total Points	600

570 and above = A
 534 - 569 = A-
 510 - 533 = B+
 492 - 509 = B
 468 - 491 = B-
 450 - 467 = C+
 420 - 449 = C
 390 - 419 = C-
 360 - 389 = D+
 330 - 359 = D
 below 330 = F

Note: **Quizzes and the final exam is cumulative**

Prerequisites - As defined in the course catalog

STATEMENT REGARDING PROFESSIONAL CONDUCT

Ferris students are expected to conduct themselves in a manner that is conducive to continued growth toward a business and/or professional career. Each student is expected to access classes regularly and to be fully prepared. All students are expected to act professionally and with a high degree of ethical conduct while applying themselves fully to the job of learning. All communications are expected to be conducted in a professional manner, whether written or oral.

It is the student's obligation to know and observe all University policies and procedures and to keep current by reading the materials posted on the Ferris University Web Site and in its printed policies and bulletins.

STATEMENT REGARDING ACADEMIC MISCONDUCT

Plagiarism, unauthorized collusion on examinations, theft, sale, purchase or other unauthorized procurement of examinations or essay material, use of unauthorized aids while taking an examination, having someone else take an exam in your place or submitting for credit any paper not written by student, taking an exam for another student, copying of "do not copy" designated library materials, copying copyrighted software and destruction of equipment by introducing a computer virus and other similar actions are considered to be academic misconduct and unacceptable for students enrolled at Ferris State University.

STATEMENT REGARDING DIVERSITY

This course embraces the Ferris Core Values of diversity by providing an environment which is supportive, safe and welcoming. We will listen respectfully to a diversity of ideas, beliefs and cultures presented by the members of the class.

Core Values

- **Collaboration:** Ferris contributes to the advancement of society by building partnerships with students, alumni, business and industry, government bodies, accrediting agencies, and the communities the University serves.
- **Diversity:** By providing a campus which is supportive, safe, and welcoming, Ferris embraces a diversity of ideas, beliefs, and cultures.
- **Ethical Community:** Ferris recognizes the inherent dignity of each member of the University community and treats everyone with respect. Our actions are guided by fairness, honesty, and integrity.
- **Excellence:** Committed to innovation and creativity, Ferris strives to produce the highest quality outcomes in all its endeavors.
- **Learning:** Ferris State University values education that is career-oriented, balances theory and practice, develops critical thinking, emphasizes active learning, and fosters responsibility and the desire for the lifelong pursuit of knowledge.
- **Opportunity:** Ferris, with a focus on developing career skills and knowledge, provides opportunities for civic engagement, leadership development, advancement, and success.

COB Syllabus Attachment is posted separately.

HSCJ 202 Principles of Information Security

Instructor: Jerry Emerick, MS, PMP, CISSP

Phone: (616) 951-4676 (mobile / preferred) or (231) 591-3148.

Email Address: Ferris Connect (Preferred) or ismjerry@yahoo.com

Office Hours: Before and After Class; Other times available by appointment.

Online Instruction: Ferris Connect / Learn (the new Ferris Connect)

Classroom: Ferris GR ATC, Thursday, 6 PM to 8:50 PM

Course Dates: October 19th to December 09, 2011

Communication – Please use Ferris Connect as your primary method of email and for submitting all assignments. I will make every attempt to return all email and phone calls within 24 hours. However, in the event you have not received a response within 24 hours please do not hesitate to reach out to me again. Assignments are due on Sunday no later than 11:59 PM. It is strongly encouraged to not wait until the weekend to contact me for assistance as there are times when I will be less available on the weekends. Email may be more effective on the weekends when necessary. I encourage office hour visits. Please don't hesitate to stop by.

Course Description

This course will be conducted in a 7 week session using both classroom and the online environments. This course will focus on providing you with insights, guidance and best practices on the principles of Information Security. We will examine the foundations of information security as defined by experts and ISC² which is considered a definitive source for Information Security best practices. We will examine Information Security using the 10 domains of knowledge as our guidebook. We will use course textbooks, other sources, and case studies to support our discussions. We will learn to apply some of the Information Security knowledge and skills through the use of group and individual activities.

Course Objectives

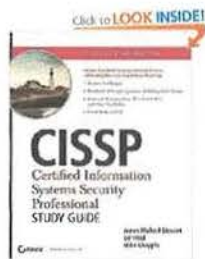
- Define and describe the concept of Information Security and its associated 10 domains of knowledge.
- Examine the key aspects of access control and its impact on Information Security.
- Explore how legal, regulatory and compliance requirement affect Information Security.
- Explore how certification and accreditation affect information security
- Recognize the need to build security into applications and network infrastructure.
- Examine the role of digital forensics in digital crime investigations.
- Define the elements of an effective incident response strategy.
- Define and apply the fundamentals of cryptography.
- Examine the impact of social engineering techniques as a threat to Information Security.
- Explore the importance preventing the entry of malicious code into the information system.
- Summarize effective security awareness principles.
- Examine the ISC² Code of Ethics.

TENTATIVE Syllabus

Course Format

This course will be conducted as a “double pace”, 7 week course. We will meet once a week in class and throughout the week in Ferris Connect for the online / web delivery portion of the class. The class will primarily consist of interactive lectures, individual assignments, and group exercises.

Course Materials



Title: CISSP Study Guide
Author: James Michael Stewart
Publisher: Sybex

Policies

Attendance and Participation - Attending class regularly and actively participating is the best way to succeed in this class. Research has shown that student attendance and participation is critical. In order to support your ability to succeed I have made attendance and participation a factor in your final grade. This should be the easiest outcome to achieve in this class. Successfully participating in class includes arriving on time, staying until the class is dismissed, not being disruptive, no excessive use of mobile phones and laptops for purposes other than taking notes, actively participating in group activities, and posting to Ferris Connect discussion topics.

Assignments - All assignments are due no later than Sunday by 11:59 PM unless otherwise stated. ALL assignments are to be submitted via Ferris Connect.

Make-up Policy - There will be no make up quizzes, exams, assignments or discussion question postings. It may be possible to pre-schedule a quiz or exam but students must contact the instructor directly and this will be determined on an individual basis.

Syllabus Changes - Adjustments to the syllabus may be necessary when it is determined that the adjustment(s) will better serve the overall learning needs of the class. We will discuss these changes together in class.

Discussions – Ferris Connect - Discussion topics may be posted on Ferris Connect during this course. Students will be required to participate and interact with one another during the semester on the course discussion boards. You are required to create at least one original reply to the instructor's discussion topic and respond to at least two of your classmates for each discussion question posted. Early posting in the Discussion will ensure you receive replies from fellow students. Your discussion posting will be graded using the following grading rubric.

TENTATIVE Syllabus
Discussion Questions Grading Rubric

Points	Description
10 points	Responded to all questions with interaction among other students. Responses began early and were often. Responses were thoughtful and topical. Outside sources, previous knowledge, and real life experience were used in responses. The flow and direction of the discussion was greatly affected by contribution.
6 to 9 points	Did not respond directly to all questions, and/or did not respond to others with comments or questions and/or all responses are made in one visit to the site. Responses lacked deep analysis or thought..
5 or less points	Minimal participation. Did not respond to all posted questions. All responses are made in one visit to the site. Responses lacked analysis or thoughtfulness (applied text or lecture teaching points or real life examples) and/or was not topical (related to the text and lectures.)
0	No participation. No response

Course Points and Grading Scale

Course Points

Grading Scale

Your performance will be assessed as follows:

Your grade will be calculated as follows:

Assessment	Total Points
Class Assignments	140
Online Assignments	200
Quizzes	90
Final	100
Participation / Attendance	70
Total Points	600

570 and above = A
 534 - 569 = A-
 510 - 533 = B+
 492 - 509 = B
 468 - 491 = B-
 450 - 467 = C+
 420 - 449 = C
 390 - 419 = C-
 360 - 389 = D+
 330 - 359 = D
 below 330 = F

Note: **Quizzes and the final exam is cumulative**

Prerequisites - As defined in the course catalog

STATEMENT REGARDING PROFESSIONAL CONDUCT

Ferris students are expected to conduct themselves in a manner that is conducive to continued growth toward a business and/or professional career. Each student is expected to attend classes regularly and to be fully prepared. All students are expected to act professionally and with a high degree of ethical conduct while applying themselves fully to the job of learning. All communications are expected to be conducted in a professional manner, whether written or oral.

It is the student's obligation to know and observe all University policies and procedures and to keep current by reading the materials posted on the Ferris University Web Site and in its printed policies and bulletins.

STATEMENT REGARDING ACADEMIC MISCONDUCT

Plagiarism, unauthorized collusion on examinations, theft, sale, purchase or other unauthorized procurement of examinations or essay material, use of unauthorized aids while taking an examination, having someone else take an exam in your place or submitting for credit any paper not written by student, taking an exam for another student, copying of "do not copy" designated library materials, copying copyrighted software and destruction of equipment by introducing a computer virus and other similar actions are considered to be academic misconduct and unacceptable for students enrolled at Ferris State University.

STATEMENT REGARDING DIVERSITY

This course embraces the Ferris Core Values of diversity by providing an environment which is supportive, safe and welcoming. We will listen respectfully to a diversity of ideas, beliefs and cultures presented by the members of the class.

Core Values

- **Collaboration:** Ferris contributes to the advancement of society by building partnerships with students, alumni, business and industry, government bodies, accrediting agencies, and the communities the University serves.
- **Diversity:** By providing a campus which is supportive, safe, and welcoming, Ferris embraces a diversity of ideas, beliefs, and cultures.
- **Ethical Community:** Ferris recognizes the inherent dignity of each member of the University community and treats everyone with respect. Our actions are guided by fairness, honesty, and integrity.
- **Excellence:** Committed to innovation and creativity, Ferris strives to produce the highest quality outcomes in all its endeavors.
- **Learning:** Ferris State University values education that is career-oriented, balances theory and practice, develops critical thinking, emphasizes active learning, and fosters responsibility and the desire for the lifelong pursuit of knowledge.
- **Opportunity:** Ferris, with a focus on developing career skills and knowledge, provides opportunities for civic engagement, leadership development, advancement, and success.

TENTATIVE Syllabus

COB Syllabus Attachment is posted separately.



Ferris State University

College of Business

COURSE: ISIN 312 Applications of Information Security

Instructor: Jerry Emerick, MS, PMP, CISSP

Phone: (616) 951-4676 (mobile / preferred) or (231) 591-3148.

Email Address: Learn Email (Preferred) or ismjerry@yahoo.com

Online Instruction: Learn (the new Ferris Connect)

Course Dates: February 29th to April 30th, 2012

Office Hours: IRC 220, 1:30 to 5:30 p.m. Thursday in Big Rapids; Email is a very good means of communicating for this course. Other times available by appointment including Learn chat or Adobe Connect meetings.

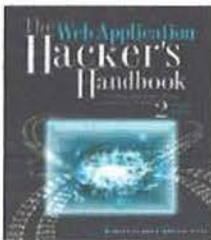
Communication – Please use Learn (new Ferris Connect) as your primary method of email and for submitting all assignments. I will make every attempt to return all phone calls within 24 hours. However, in the rare event you have not received a return call within 24 hours please do not hesitate to reach out to me again. All assignments are due on Sunday no later than 11:59 PM. It is strongly encouraged to not wait until the weekend to contact me for assistance as there are times when I will be less available on the weekends. Email may be more effective on the weekends when necessary. I encourage office hour visits. Please don't hesitate to stop by.

Prerequisites – As defined in the course catalog

Course Description

This course will be conducted in an online environment using Learn. Students apply the tools and concepts of information security in the context of Internet web applications. Students will analyze web application architecture, tools, and technologies. Students will examine common web application vulnerabilities, how to discover and exploit vulnerabilities, and how to prevent these flaws and vulnerabilities. Students will also apply attack methods for common web application vulnerabilities using ethical hacking and penetration testing techniques.

Required Course Materials



Title: The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws

Author: Dafydd Stuttard

Publisher: Wiley; Second Edition

ISBN: 1118026470

Course Methods and Objectives

Course Methods

- Online Lectures and Presentations
- Audio / Video Demonstrations
- Assignments and Projects
- Discussion Forum
- Quizzes
- Final Exam

Course Objectives

It is my expectation that you will be able to do the following upon completion of this course:

- Analyze and accurately describe web application architecture including the role of the client / browser, web server, database server, and network components
- Examine and accurately describe web application technologies including HTTP, HTTPS, cookies, and sessions
- Map web application content and functionality
- Install, configure, and execute an intercepting proxy to analyze and manipulate web application content
- Apply attack methods such as Cross Site Scripting and SQL Injection to expose web application vulnerabilities
- Analyze methods to remove web application vulnerabilities that you have exposed
- Demonstrate an ability to utilize components of a web application vulnerability toolkit and methodology to perform web application penetration testing.

Assignments

All assignments will be posted on Learn. All assignments are due Sunday of each week by 11:59 PM unless otherwise stated.

Assessments

There will be quizzes and a final exam. The assessments are cumulative. They are a combination of multiple choice, true / false, and short essay questions.

For this online class, exams will be open-book and open-notes

Discussion Threads

Discussions –Discussion topics will be posted on Learn during this course. Students will be required to participate and interact with one another during the semester on the course discussion boards. You are required to create at least one original reply to the instructor's discussion topic and respond to at least two of your classmates for each discussion question posted. You must also participate in the discussion more than once during the week. **Waiting until Sunday to begin your participation in the discussion will result in lost points.** Early posting in the Discussion will ensure you receive replies from fellow students. Your discussion posting will be graded using the following grading rubric.

Discussion Questions Grading Rubric

Points	Description
25 points	Responded to all questions with interaction among other students. Responses to other students began early and occurred at least twice during the discussion in multiple visits to the course site . Responses were thoughtful and topical. Outside sources, previous knowledge, and real life experience were used in responses. The flow and direction of the discussion was greatly affected by contribution.
15 to 20 points	Did not respond directly to all questions, and/or did not respond to others with comments or questions and/or all responses are made in one visit to the site. Responses lacked deep analysis or thought.
15 or less points	Minimal participation. Did not respond to all posted questions. All responses are made in one visit to the site. Responses lacked analysis or thoughtfulness (applied text or lecture teaching points or real life examples) and/or was not topical (related to the text and lectures.)
0	No participation. No response

Policies

Assignments - All assignments are due Sunday by 11:59 PM unless otherwise stated. **ALL assignments are to be submitted via Ferris Connect.**

Make-up Policy - There will be no make-up quizzes, exams, or discussion question postings. It may be possible to pre-schedule a quiz or exam but students must contact the instructor directly and this will be determined on an individual basis. **Late assignments and projects will be docked 10% per day for each day they are late without exception.**

Syllabus Changes - Adjustments to the syllabus may be necessary when it is determined that the adjustment(s) will better serve the overall learning needs of the class.

Course Points and Grading Scale

Course Points

Your performance will be assessed as follows:

Assessment	Total Points
Assignments and Projects	300
Discussion Topics	175
Self-Assessment	25
Quizzes	100
Final Exam	100
Total Points	700

Grading Scale

Your grade will be calculated as follows:

95% and above = A
90% - 94% = A-
88% - 89% = B+
85% - 87% = B
80% - 84% = B-
78% - 79% = C+
75% - 77% = C
70% - 74% = C-
68% - 69% = D+
65% - 67% = D
60% - 64% = D
below 60% = F

Note: The quizzes and final exam are cumulative

STATEMENT REGARDING PROFESSIONAL CONDUCT

Ferris students are expected to conduct themselves in a manner that is conducive to continued growth toward a business and/or professional career. Each student is expected to access classes regularly and to be fully prepared. All students are expected to act professionally and with a high degree of ethical conduct while applying themselves fully to the job of learning. All communications are expected to be conducted in a professional manner, whether written or oral.

It is the student's obligation to know and observe all University policies and procedures and to keep current by reading the materials posted on the Ferris University Web Site and in its printed policies and bulletins.

STATEMENT REGARDING ACADEMIC MISCONDUCT

Plagiarism, unauthorized collusion on examinations, theft, sale, purchase or other unauthorized procurement of examinations or essay material, use of unauthorized aids while taking an examination, having someone else take an exam in your place or submitting for credit any paper not written by student, taking an exam for another student, copying of "do not copy" designated library materials, copying copyrighted software and destruction of equipment by introducing a computer virus and other similar actions are considered to be academic misconduct and unacceptable for students enrolled at Ferris State University.

STATEMENT REGARDING DIVERSITY

This course embraces the Ferris Core Values of diversity by providing an environment which is supportive, safe and welcoming. We will listen respectfully to a diversity of ideas, beliefs and cultures presented by the members of the class.

Core Values

- **Collaboration:** Ferris contributes to the advancement of society by building partnerships with students, alumni, business and industry, government bodies, accrediting agencies, and the communities the University serves.
- **Diversity:** By providing a campus which is supportive, safe, and welcoming, Ferris embraces a diversity of ideas, beliefs, and cultures.
- **Ethical Community:** Ferris recognizes the inherent dignity of each member of the University community and treats everyone with respect. Our actions are guided by fairness, honesty, and integrity.
- **Excellence:** Committed to innovation and creativity, Ferris strives to produce the highest quality outcomes in all its endeavors.
- **Learning:** Ferris State University values education that is career-oriented, balances theory and practice, develops critical thinking, emphasizes active learning, and fosters responsibility and the desire for the lifelong pursuit of knowledge.
- **Opportunity:** Ferris, with a focus on developing career skills and knowledge, provides opportunities for civic engagement, leadership development, advancement, and success.

STATEMENT REGARDING DISABILITIES

Ferris State University is committed to following the requirements of the Americans with Disabilities Act Amendments Act and Section 504 of the Rehabilitation Act. If you are a student with a disability or think you may have a disability, contact the Disabilities Services office at 231.591.3057 (voice), or email ecds@ferris.edu to discuss your request further. More information can be found on the web at <http://www.ferris.edu/htmls/colleges/university/disability/>.

Any student registered with Disabilities Services should contact the instructor as soon as possible for assistance with classroom accommodations.

COB Syllabus Attachment is posted separately.



Ferris State University

College of Business

COURSE: PROJ 320 Project Management

Instructor: Jerry Emerick, MS, PMP, CISSP

Phone: (616) 951-4676 (mobile / preferred) or (231) 591-3148.

Email Address: Ferris Connect (Preferred) or ismjerry@yahoo.com

Online Instruction: Ferris Connect / Learn (the new Ferris Connect)

Course Dates: January 9th to May 4th, 2012

Office Hours: IRC 220, 1:30 to 5:30 p.m. Thursday in Big Rapids; Email is a very good means of communicating for this course. Other times available by appointment including Ferris Connect chat.

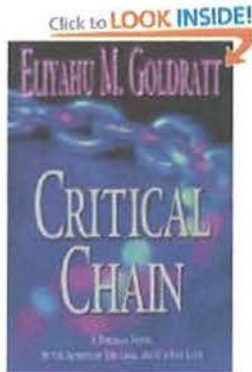
Communication – Please use Ferris Connect as your primary method of email and for submitting all assignments. I will make every attempt to return all phone calls within 24 hours. However, in the rare event you have not received a return call within 24 hours please do not hesitate to reach out to me again. All assignments are due on Sunday no later than 11:59 PM. It is strongly encouraged to not wait until the weekend to contact me for assistance as there are times when I will be less available on the weekends. Email may be more effective on the weekends when necessary. I encourage office hour visits. Please don't hesitate to stop by.

Course Description

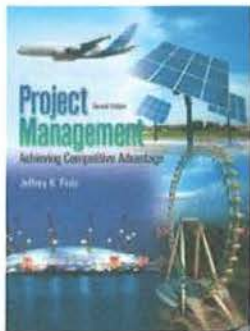
This course will be conducted in an online environment using Ferris Connect. It will focus on providing you with insights, guidance and best practices on the art and science of project management. We will examine the foundations of project management as defined by experts including Eliyahu Goldratt and the Project Management Institute. We will review the various aspects of the project management lifecycle and knowledge areas and use resources such as the Project Management Body of Knowledge, the course textbooks, and case studies to support our discussions. We will learn to apply some of the project management knowledge and skills through the use of activities and the preparation of project management plans covering various topics. We will also introduce project management career paths and provide a basic introduction to project management software tools.

Prerequisites - As defined in the course catalog

Required Course Materials



Title: Critical Chain
Author: Eliyahu Goldratt
Publisher: North River Press
ISBN: 0884271536



Title: Project Management: Achieving Competitive Advantage
Author: Jeffrey Pinto
Publisher: Prentice Hall
ISBN: 0136065619

Recommended Course Materials



Title: Project Management Body of Knowledge (PMBOK)
4th Edition
Author: Project Management Institute
Publisher: Project Management Institute
ISBN: 978-1933890517

Course Methods and Objectives

Course Methods

- Online Lectures and Presentations
- Discussion Forum
- Individual Assignments
- Group Project Plan
- Midterm and Final Exams

Course Objectives

- The student will examine project management knowledge areas and apply that knowledge in the preparation of project documents, deliverables, and team work.
- The student will evaluate project management best practices and assess their effectiveness and value through practice assignments and collaborative discussion.
- The student will work within a team to develop a comprehensive project plan focused on managing a successful project throughout its life cycle.
- The student will apply the Project Management Institute's Code of Ethics and Professional Responsibility and apply the code to various scenarios common in project management.
- The student will evaluate their need to further develop interpersonal skills such as communication, conflict management, leadership and team building through practice scenarios with other students.

Assignments

All assignments will be posted on Ferris Connect. All assignments are due Sunday of each week by 11:59 PM unless otherwise stated.

Mid-Term and Final

There will be a mid-term and final exam. The exams are cumulative. They are a combination of multiple choice and short essay questions.

For this online class, exams will be open-book and open-notes

Discussion Threads

Discussions – Ferris Connect - Discussion topics will be posted on Ferris Connect during this course. Students will be required to participate and interact with one another during the semester on the course discussion boards. You are required to create at least one original reply to the instructor's discussion topic and respond to at least two of your classmates for each discussion question posted. You must also participate in the discussion more than once during the week. **Waiting until Sunday to begin your participation in the discussion will result in lost points.** Early posting in the Discussion will ensure you receive replies from fellow students. Your discussion posting will be graded using the following grading rubric.

Discussion Questions Grading Rubric

Points	Description
10 points	Responded to all questions with interaction among other students. Responses began early and were often. Responses were thoughtful and topical. Outside sources, previous knowledge, and real life experience were used in responses. The flow and direction of the discussion was greatly affected by contribution.
6 to 9 points	Did not respond directly to all questions, and/or did not respond to others with comments or questions and/or all responses are made in one visit to the site. Responses lacked deep analysis or thought..
5 or less points	Minimal participation. Did not respond to all posted questions. All responses are made in one visit to the site. Responses lacked analysis or thoughtfulness (applied text or lecture teaching points or real life examples) and/or was not topical (related to the text and lectures.)
0	No participation. No response

Policies

Assignments - All assignments are due Sunday by 11:59 PM unless otherwise stated. **ALL assignments are to be submitted via Ferris Connect.**

Make-up Policy - There will be no make-up quizzes, exams, or discussion question postings. It may be possible to pre-schedule a quiz or exam but students must contact the instructor directly and this will be determined on an individual basis. **Late assignments will be docked 10% per day for each day they are late** without exception.

Syllabus Changes - Adjustments to the syllabus may be necessary when it is determined that the adjustment(s) will better serve the overall learning needs of the class.

Course Points and Grading Scale

Course Points

Your performance will be assessed as follows:

Assessment	Total Points
Course Status Reports (7 @ 5 points)	35
Individual Assignments	160
Group Assignments	110
Self-Assessment	25
Mid-Term Exam	50
Final Exam	100
Discussion Threads (12 @ 10 points)	120
Total Points	600

Note: **The mid-term and final exams are cumulative**

Grading Scale

Your grade will be calculated as follows:

570 and above = A
534 - 569 = A-
510 - 533 = B+
492 - 509 = B
468 - 491 = B-
450 - 467 = C+
420 - 449 = C
390 - 419 = C-
360 - 389 = D+
330 - 359 = D
below 330 = F

STATEMENT REGARDING PROFESSIONAL CONDUCT

Ferris students are expected to conduct themselves in a manner that is conducive to continued growth toward a business and/or professional career. Each student is expected to access classes regularly and to be fully prepared. All students are expected to act professionally and with a high degree of ethical conduct while applying themselves fully to the job of learning. All communications are expected to be conducted in a professional manner, whether written or oral.

It is the student's obligation to know and observe all University policies and procedures and to keep current by reading the materials posted on the Ferris University Web Site and in its printed policies and bulletins.

STATEMENT REGARDING ACADEMIC MISCONDUCT

Plagiarism, unauthorized collusion on examinations, theft, sale, purchase or other unauthorized procurement of examinations or essay material, use of unauthorized aids while taking an examination, having someone else take an exam in your place or submitting for credit any paper not written by student, taking an exam for another student, copying of "do not copy" designated library materials, copying copyrighted software and destruction of equipment by introducing a computer virus and other similar actions are considered to be academic misconduct and unacceptable for students enrolled at Ferris State University.

STATEMENT REGARDING DIVERSITY

This course embraces the Ferris Core Values of diversity by providing an environment which is supportive, safe and welcoming. We will listen respectfully to a diversity of ideas, beliefs and cultures presented by the members of the class.

Core Values

- **Collaboration:** Ferris contributes to the advancement of society by building partnerships with students, alumni, business and industry, government bodies, accrediting agencies, and the communities the University serves.
- **Diversity:** By providing a campus which is supportive, safe, and welcoming, Ferris embraces a diversity of ideas, beliefs, and cultures.
- **Ethical Community:** Ferris recognizes the inherent dignity of each member of the University community and treats everyone with respect. Our actions are guided by fairness, honesty, and integrity.
- **Excellence:** Committed to innovation and creativity, Ferris strives to produce the highest quality outcomes in all its endeavors.
- **Learning:** Ferris State University values education that is career-oriented, balances theory and practice, develops critical thinking, emphasizes active learning, and fosters responsibility and the desire for the lifelong pursuit of knowledge.
- **Opportunity:** Ferris, with a focus on developing career skills and knowledge, provides opportunities for civic engagement, leadership development, advancement, and success.

COB Syllabus Attachment is posted separately.

ISIN 300 – Link and Visual Analysis

Tentative Syllabus - Instructor reserves right to modify when deemed appropriate

Instructor: Greg Gogolin, Ph.D.

Work/Phonemail: (231) 591-3159 (FSUConnect e-mail preferred)

e-mail: Please use FSUConnect (ismgreg@yahoo.com is a backup email address)

Office hours: By appointment.

Prerequisites: none.

Text

No Place To Hide – O’Harrow – ISBN 9780743254809

Tentative Schedule

Class meets March 15 – April 30 in ATC 145. Course website in FerrisConnect.

Course Format

This course will include a combination of hand’s-on, analysis, discussion, team and individual work. The goal is to develop skills and understanding related to the critical issues surrounding information analysis.

Course Outcomes

Upon completing this course, students will be able to:

1. Describe and apply the visual analysis and investigative process.
2. Construct a visual analysis environment for data investigation.
3. Demonstrate how to utilize a visual analysis environment for information interpretation.
4. Evaluate and interpret temporal and associative characteristics of information.
5. Discuss the history of intelligence and major events that have shaped it.

Assignments: All assignments/projects must be turned in via FSUConnect using 12 point Times New Roman, Arial or Georgia font. Headings may be larger font and/or bold. Assignments turned in by other means will not be accepted.

Deliverable	Description	Max Point Value	Due Date
i2/visual analysis research paper	Detailed in FSUConnect	10	March 23
No Place to Hide reaction paper	Detailed in FSUConnect	10	March 26
Self i2 Chart	Discussed and completed in class	5	March 23
Exercise 1 – Drugs (embedded objects and attributes)	Class exercise	5	March 30
Exercise 2 – Buys (presentations)	Class exercise	5	April 6
Exercise 3 – Surveillance (Theme lines)	Class exercise	5	April 13
Exercise 4 – Timeline (temporal analysis, customization)	Class exercise	5	April 13
Mid-Term Exam	In Class	10	April 5

Exercise 5 - Phone (importing)	Detailed in FSUConnect	5	April 13
Research topic of choice and presentation	To be arranged with instructor by April 5. (student responsibility to meet with instructor to discuss topic - team)	10	April 19
Class Case	Team Exercise -- detailed in FSUConnect.	20	April 27
Final Exam	In Class	10	May 3

Case:

There is one case for this course. For Spring 2010, the class case will be season 1 of The Wire. The case will be developed in class and away from class. Student teams will prepare visual analysis of the case using i2 Analyst Notebook and any other tools necessary to support this analysis.

Exercises:

All exercises will be discussed in class and work for each exercise may be performed in the lab during class if time permits. Each is detailed in FSUConnect. These exercises are to be done individually.

I2/Visual Analysis:

Detailed in FSUConnect.

Research topic of choice:

This must be arranged individually with the instructor by 4/5. Topics should be related to visual analysis. This is an individual effort by the student.

Tests:

The final exam in FerrisConnect must be completed by May 3.

Grading

Percent	Grade
93-100	A
90-92	A-
88-89	B+
83-87	B
80-82	B-
78-79	C+
70-77	C
<70	F

Course Notes:

Students must conduct themselves in a professional manner at all times. Audible cell phones, pagers or similar electronic devices are not permitted in class. Interruptions will result in point deduction. Email shall not be accessed during instruction time. Remember – typing and other activities can be distracting to your classmates. Due dates must be adhered to. Late assignments will not be accepted. **No projects or course work will be accepted after posted due dates.** Grades will be posted in FSUConnect approximately 1 week after they are due. There will be no grade changes after the semester ends. Frequent interaction in the course is expected. Students missing more than one session of class will not pass the course. Extenuating circumstances or unforeseen events will be handled at the discretion of the instructor and arrangements must be made prior to the absence. To pass this course, all assignments must be the original work of the student or team. Plagiarism is fraud and will be referred to Judicial Services. Students must have completed at least 80% of course material to receive an incomplete. Any student who feels s/he may need an accommodation based on the impact of a disability should contact me

privately to discuss your specific needs. Please contact the Disabilities Services Office, Arts and Sciences Commons, 1017k, (231) 591-3772 to coordinate reasonable accommodations for students with documented disabilities. Instructor reserves the right to make modifications to the course or this syllabus to accommodate unforeseen circumstances. The dates in this syllabus supersede any discrepancies from any other source. Contact the instructor via FSUConnect email for questions regarding class materials or assignments with sufficient lead time. Your failure to plan is not the instructor's crisis.

Outline:

Module 1:

Intro

Icebreaker – what is something cool that you did

Course policies

Explain Visual Analysis

Go through about self

7 entity types

Superman's world

JFK

All calls final - timeline with 4 call records

Entity Matching Example

Media

Projects –

1) self

2) handouts

3) The Wire

Go through surveillance video – the wire

Watch episode 1

Who, what, when, where, why, how

Module 2:

Visual Intelligence and Actionable Intelligence

I2 media – counter terrorism, analyst notebook, chart reader

Walkthrough I2 and developing standards

About Me

Relational Database overview

- tables

- indexes, keys

- data types

Work time

Assignment

Module 3:

Teams

Intelligence content prior to going into tool material

Charts have 3 components –

- entities

- links
- attributes

Links –

- links represent an association bt. 2 entities on a chart
- edit the properties to make them more meaningful
- can choose which parts of information to display on the chart
- can specify strength
 - o reliability
 - show how to specify strength
- can specify direction
 - o arrow head(s)
 - show how to add/reverse arrowheads

Attributes –

- show characteristics of items on your chart.
- Can be added to all chart items
- Typically show below the icon

** Identity is the key for attributes.

- Who is King? Elvis.
- What is King? Identity.
- Spaces are valid characters
- Merged charts recognize identities
 - o Merge by drag and drop

* Make identity naming standards – i.e., the address is identity for house

4 types of attribute classes

- text – for a description. Example – cocaine was the drug seized
- number – for a value – Example – a person's age
- time – date and time
- flag – a yes/no value – Example – person has criminal record

Attribute instance –

- add an attribute class to an item and enter a value
- add an attribute entry with a fixed value to an item.

(add a person from the people template to a chart. Drag an attribute entry to the icon).

Attribute Bar –

- add a person from the template to a chart. Select nationality from the attribute bar drop down. Enter British. Click add attribute arrow.
- Adds to all the icons that are selected.
- Show how to drag more than one attribute at a time to the icon.

Another way to add attributes -

- Double click icon
- Click Add button

Change attribute value –

- Double click icon
- Double click value column and edit

Add attribute class –

- Format
- Attribute Classes
- New
- Enter new class and select which palette to have it appear in.

?? How to have attributes not displayed ??

- Format
- Attribute Classes
- Edit the attribute
- Toggle off the display on chart check box

Have people create a temp chart, add attributes, change values, add an attribute class

?? How to have attributes not displayed ??

- Format
- Attribute Classes
- Edit the attribute
- Toggle off the display on chart check box

Grades of information

- provides an indication of quality of the information
- format, entity types, grading system
- never change grading system when chart is empty
- order of grading is important
- Grade 1 – reliability rating of the source
 - o Reliable
 - o Sometimes reliable
 - o Unreliable
 - o Untested
- Grade 2 – privacy ratings of information
 - o Confidential
 - o Signature required
 - o Unrestricted
- Grade 3 – reliability of information
 - o Reliable information
 - o Unreliable
 - o Unknown quality

Source of information

- lists sources for the information
- o Witness
- o Informant
- o Officer
- o Record

Cards –

- units you can create for standard info desc.
- a bio card has ht, wt, eye color, etc. (I'm thinking these might be better served using attributes)
- use cards rather than desc. and grades – better for analysis/reporting

OLE object –

- can link to an object
 - o linked to chart but not saved in it
 - o need to make sure link is accessible
 - o if document is updated, new document will appear on chart
 - o chart size stays the same
- embed object in chart
 - o a copy of the original is stored in chart
 - o changes to original not reflected in chart
 - update manually
 - o chart size increase by size of object

To add OLE object to chart as link –

- Insert OLE Object, Documents, Document, Create from File, Browse to file, Open, 'Display as Icon' to show the transcript as an icon. If you don't choose display as icon, entire transcript will be displayed on chart. Turn on the **Link** checkbox to make a link between chart and original.

To add OLE object to chart as embedded item –

- Insert OLE Object, Documents, Picture, Create from File, Browse.
 - o If you want picture to be framed with a border, right click on picture and select Display, Border.

?? why don't icons display in chart

Class exercise –

- 1) link an object, embed and object, create object during link/embed process, cards, attributes, new attributes, setting time on timeline, reports, merge

1 level of undo (undo is alt + back – in windows it is alt + Z)

Make backup copies of charts

<=? - click on this box and then click on icon for help.

Charts have 3 components –

- entities
- links
- attributes

Insert box – used to group entities

- put entities on chart and then place ‘insert box’ on entities

Picture –

- link doesn’t store media
- embedded picture stores media in workbench chart

Timeline –

- to stop timeline from extending on each insert, dbl click, style, display, leftmost/rightmost chart items

There are 7 entities. They differ only by visual appearance. They hold the same info.

- there are 4 folders in the properties area
- * name entity first name lower case last name upper case i.e., DanRIVERA
- * date and time almost always goes on link – not entity
- in desc. field, for people put in things like ht, wt, eye color, hair
- Grade 1 for organization
- Grade 2 for the info
- Grade 3 type of info
- Source – blinks, so you can type in something not in selection dropdown.

Module 4:

Intelligence –

- business intelligence
- competitive intelligence
- other types

Forensic tools for surveillance

- computer
- video
- other means
- <http://www.wired.com/politics/law/news/2002/01/50036>

What would you have in a digital forensic tool kit?

Forensic process –

- repeatable and get same result
- false negatives
- false positives

Teams –

- how do you work in a team environment?
- What makes the team effective?
- What makes a team ineffective?
- experiences

Visual Analysis –

Class discussion –

- what is VA?
- What technologies for VA exist?
- What are the applications of VA?
- Who uses VA and how?
- Who are the VA vendors and what are their products?

Breakouts – teams to research and present

Skill of week is building relational analysis charts and merging charts.

Too many icons can make a chart hard to visualize. Sometimes a new representation of multiple icons can present a stronger image.

Person entity and bldg entity – draw owner link, then click on bldg, tools, change representation – box. Then place the person entity in the box. You may even shade the box.

--

Transaction links – change color of text, not line or won't be a transaction anymore. It will be that color. So will lose track of when sorting links.

To change properties of multiple entries, ctl click entities, right click and choose combined properties

Merge Charts

Relational analysis

Timeline

To change to themeline –

- select all
- tools
- change representation

- theme line and add order to all chart...

Click layout setup icon to modify theme line layout.

Module 5:

Review of Questions
 Discuss mid-term options
 Case
 Controlled Buys

Module 6:

Questions and discussion on The Wire and teams
 How to customize Entities and add Attribute Classes
 Walk through themelines and event frames
 Exercise 3 – Surveillance

Module 7:

What I'd like you to do this week is review for the final and make sure all of your assignments are in.
 I've created a podcast to help you review for the midterm. It is at <http://web.mac.com/ismgreg/iWeb/ISM/HSCJ315/HSCJ315.html>
 Note that the url is case sensitive, so cut and paste the link into your browser. Also, make sure your speakers are on.

Module 8:

View episode 5. Map episodes 3-5 of The Wire

Module 9:

Importing

- 2 file types
 - o Txt (default)
 - o Csv
- Data should be clean, consistent, converted

(penlink is phone data)

%date, time, destination, destination #, duration ← record description

↑

Percent is initial character – import process will skip this record and go to next

Need an A to B relationship and it should match the record description

Import

- browse for field
- example button (check alignment)
- choose date and time formats

When creating import spec – if answer not in example box extracted fields then you are looking for a value.

Entity A	Link	Entity B
----------	------	----------

Representation – icon	Multiplicity – single	Representation – icon
Type – telephone	Type – telephone call	Type – telephone
Identifier – 3055135260 (value)	Label – default (occurrences)	Identifier – column A (field 1)
Label – HADEN	Direction – default (A to B)	Label – default (same as Identifier)
Date – nothing (no date on entity)	Strength – default (confirmed)	Date – nothing (no date on entity)
Time – nothing (no time on entity)	Date – field 2	Time – nothing (no time on entity)
	Time – field 3	
	Width - linear	
	Attribute – duration – field 4 (class value – type in “duration”. Class duration, type number, value is the field)	

** don't forget to strip characters and spaces

--

To total or select items on a chart –

- list items, sort by criteria, highlight your items (then they will be highlighted on chart)

**When putting in pictures, choose picture (toolbar icon), entity type (for example, male), and then browse for picture. This will give the picture the entity type.

To change to themeline –

- select all
- tools
- change representation
- theme line and add order to all chart...

Click layout setup icon to modify theme line layout.

For readability

- put date and time on phone link
- remove # if multiplicity (they are all 1)

Select all

- click on a phone
- go to links, display – select date time, deselect label
- edit chart properties
 - o go to attribute class (will have a duration if created in import spec). May need to edit the attribute and put in a prefix/suffix for display.

***Tip – hold alt key and left click and drag labels.

- 1) icons, grouped, single multiplicity
- 2) multiple, multiplicity

To change icon to picture –

- place OLE pic on chart
- it is still selected
- clt and select entity you want to replace
- tools, merge entities

** To copy an import spec –

- Tools, options, paths
- can select importer.imp and send to
- use load button on import into

To best sort through phone data, list items and highlight #'s with names.

** Event – if using description of date and time rather than Date: and Time: you need to use just Desc. Use one or the other, not both.

*Tip – to change all of the same entities properties –

- analysis list items
- select all
- rt click on a cursor
- change properties
- can only change all properties (combined properties) if same type of entity
- ctl + A won't work because selecting all entities and they might be different.

Module 10:

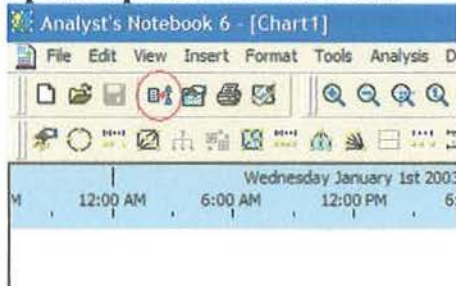
To import data, you need to specify what the data layout is. If you fill out this import specification, it is an easy process.

DEBOS

Entity A	Link	Entity B
Representation – icon	Multiplicity – single	Representation – icon
Type – telephone	Type – telephone call	Type – telephone
Identifier – 7865551163	Label – default (occurrences)	Identifier – column D (field 4)
Label – DEBOS	Direction – default (A to B)	Label – default (same as Identifier)
Date – nothing (no date on entity)	Strength – default (confirmed)	Date – nothing (no date on entity)
Time – nothing (no time on entity)	Date – field 3	Time – nothing (no time on entity)
	Time – field 1	
	Width - linear	
	Attribute – duration – field 2 (change field to value and call it duration. This is the class. Class, type, value.	

After you have filled this out, you need to enter this information into i2. The following information is how to enter into i2. This is a copy of an i2 document that I received from Dan Riveria at i2.

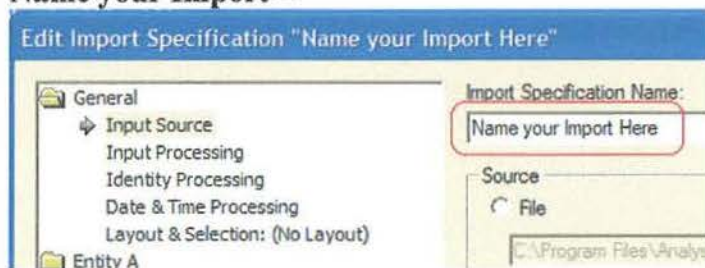
Open Importer from tool bar -



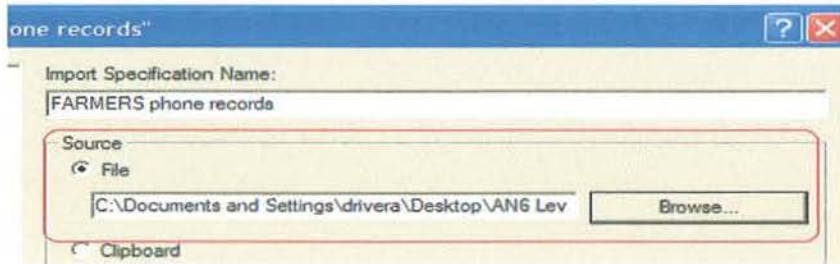
Select 'New' to begin -



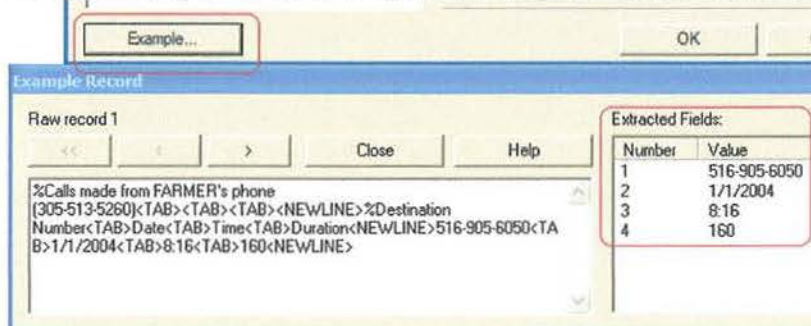
Name your Import -



Select 'File' radio button and use the 'Browse' to find the document on your system

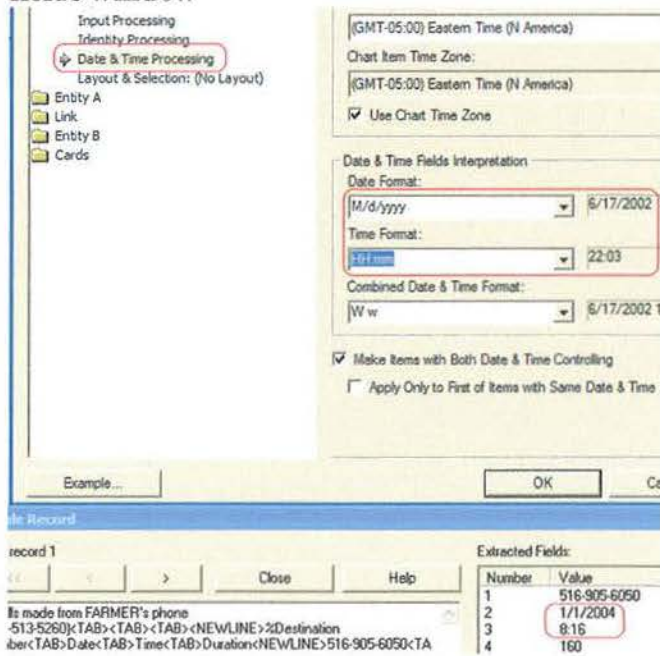


Select 'Example' button to open 'Example Record' window



Insure that the information in the 'Extracted Fields' window appears vertically and in numerical order

Go to 'Date and Time Processing' and set both to match the format in the extracted fields window



Select desired layout



Enter 'Entity A' values;

REPRESENTATION reflects the type of entity to be used

TYPE reflects the specific icon to be used

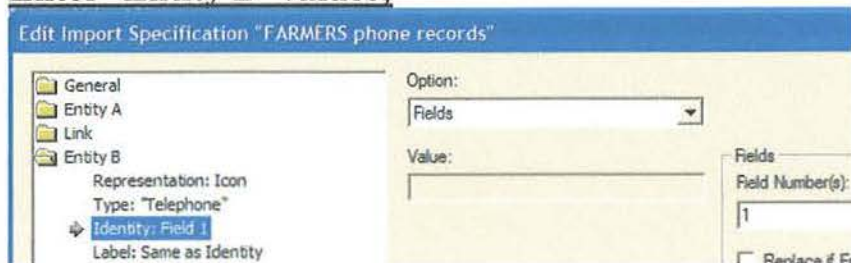
IDENTITY reflects the unique identifier of the entity

LABEL can be same as identity



***NOTE** When the value is static, the 'Option' is 'value'
When the value is found in an 'extracted field', the 'Option' is 'field'

Enter 'Entity B' values;



Enter 'Link' values

MULTIPLICITY:

*Single = One link with total number of occurrences on label

*Directed = One link with total number of occurrences in each direction (requires mapping)

*Multiple = One link for each individual occurrence

TYPE reflects the type of link

LABEL can be left on default (Occurrences)

DATE - choose respective field

TIME – choose respective field

General
Entity A
Link
Multiplicity: Single
Type: "Telephone Call"
Label: Occurrences
Direction: "Entity A --> Entity B"
Strength: "Default"
Date: Field 2
Time: Field 3

Option:
Fields
Value:
00:00

Fields
Field 1
3

Select 'OK'

OK Cancel Help

Select 'Run'

Import Into: "Chart1"

Input Specifications:
Name
FARMERS Phone records

OK
Cancel
Help

New... Duplicate Edit... Watch
Delete Load... Run

Select 'OK'

Import Into: "Chart1"

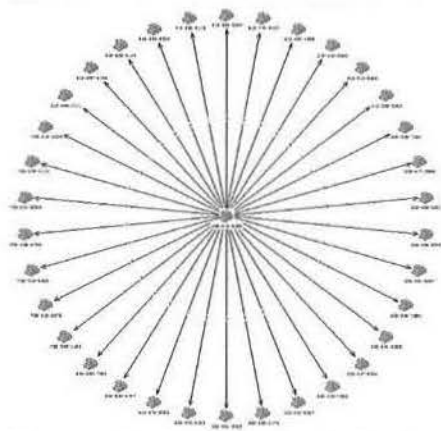
Input Specifications:
Name
FARMERS Phone records

OK
Cancel
Help

New... Duplicate Edit... Watch
Delete Load... Run

12:00 AM

Select 'Fit chart in window'



Module 11:

- Create import specs - themeline
- Adjust themeline by dragging entities
- Add attribute class (suspect)
- List Items
- Copy to XL

Grouped by Time - Analysis, Layout Chart Setup

HSCJ315: Advanced Digital Forensics and Incident Response Spring Semester 2012

Professor Gogolin contact information:

Office: IRC 212g

Phone: 231-591-3159 (office)

Email: Use Ferris Connect email. An alternate email is ismgreg@yahoo.com Email is generally the most efficient means of communication. Please include your name and course number in any communications with me (email, voice mail, etc.).

Office Hours: Monday 3:00pm - 6:00pm and by appointment

Required Text: EnCase Computer Forensics: The Official EnCase Certified Examiner Study Guide (with DVD) by Steve Bunting (ISBN:0470181451)

Course Credits: 3

Course Prerequisites: HSCJ310

Course Description: Students explore advanced digital forensic techniques and develop skills to deal with situations requiring a sophisticated response. Emerging and next generation computer technologies and threats as well as proactive security measures and threat prevention will also be investigated. Students will utilize several digital forensic tools and techniques for surveillance, gathering evidence, and-or crime scene reconstruction for incidence processing.

Ethics Statement: The technologies, situations and implications that comprise the field of digital forensics require the highest ethical and moral standing. As such, any personal lapse of this standing – whether it is a lapse in judgment or a well constructed scheme – may constitute grounds for dismissal from the course, the program, and Ferris State University. Additionally, there is potential for legal consequence that may include prosecution. Do not duplicate or continue to access any information that may be of a criminal nature, violates privacy, and/or conflicts with this Ethics Statement. Should you come across anything of this nature don't hesitate to contact either Dr. Gogolin immediately.

Course Policies: This syllabus is tentative in nature and may be modified by the instructor at any time. Assignments must be submitted in RTF or PDF format by the due date to FerrisConnect. Late work will not be accepted unless warranted by a documented emergency. No projects or course work will be accepted after 4/28/12 unless prior arrangements have been made. Grades will be posted in FerrisConnect approximately 1 week after assignments are due. There will be no grade changes after the semester ends. Submitted work may be checked using SafeAssign or similar services. If you object to having your work submitted to such services, you must notify the instructor via email no later than 3/17/12. Attendance and participation in all class meetings is required. Students missing more than 1 week of course interaction will not pass the course. Extenuating circumstances or unforeseen events will be handled at the discretion of the instructor and arrangements should be made prior to the absence. To pass this course, all assignments must be the original work of the student or team. All references and use of external sources must be appropriately documented. Plagiarism will result in not passing the course. Students must have completed at least 80% of course material and a completion contract to receive an incomplete. Any student who feels s/he may need an accommodation based on the impact of a disability should contact the instructor privately to discuss your specific needs. Please contact the Disabilities Services Office, Arts and Sciences Commons, 1017k, (231) 591-3772 to coordinate reasonable accommodations for students with documented disabilities. Cell phones should be silenced during class meetings; breaks will be provided during which calls may be made. Use of a computer for reasons not related to course activities may result in loss of points. The Instructor

HSCJ 317 – Fraud Examination
Syllabus
Online
Summer, 2010 June 30 – August 11 Fully ONLINE

Instructor: Doug Blakemore, Ph.D.
Contact Info: ismdoug@yahoo.com
Phone: 231-832-9657 (home) - Preferred
Google phone: 231-680-0596

Office Hours: By appointment or via FSU VISTA email, chat or phone

Text: Corporate Fraud Handbook: Prevention and Detection by Joseph Wells,
second Edition ISBN 978-0-470-0951-1

Course Description

Students will examine the fundamental reasons of why people commit fraud. Participants will investigate and explore how opportunity, pressures and rationalization are linked together to foster an atmosphere that can allow fraud to occur. Additionally, students will learn basic examination techniques for discovering fraud and more importantly, how to deter fraud from taking place.

Course Objectives

Upon completing this course, students will be able to:

- Identify and describe various forms of employee and financial statement fraud.
- Identify and describe procedures, checks and balances and other methods of preventing fraud.
- Investigate methods of collecting and handling evidence including interviewing techniques, auditing books
- Identify and describe corruption in the form of conflict of interest and bribery in the corporate environment.

RESEARCH

When conducting research, students are strongly encouraged to make use of the Ferris Library for Information Technology and Education (FLITE) Off Campus Database Access. For more information, visit <http://library.ferris.edu/proxysetup.html>

All written assignments must be in MS Word.doc or in Rich Text (RTF) format and conform to APA style in regards to:

- having a cover page which includes:
 - Your name
 - The University
 - Class
 - Student ID
 - Assignment #
 - Date

(See example later in this syllabus)

Assignments missing the title page will lose points.

- document must be double spaced
- document must be LEFT justified (never full justified)
- first lines of paragraphs are to be indented to the first tab stop (unless a long quote) then indent first line of paragraphs a second tab stop as per APA rules.
- all uses of other people's work must be cited and referenced.
- All assignments must be the original work of the student/team.
- Please read Ferris State University's Academic Policy Information/Academic Honesty.

Plagiarism: Plain and simple. If you use ANYONE's work – regardless if it is a direct quote or paraphrase – then you MUST reference it. FAILURE TO REFERENCE it will result in my assuming you represented that person's work as your own and therefore stole it. Results will be failure of the work with no possible ability to make up the work. The second time in the course you are caught, it will be an automatic failure of the course.

Each student must demonstrate proficiency in the use of the English language in all work submitted for this course. Grammatical errors, spelling errors, and writing that do not express ideas clearly will affect your grade. The professor will not provide remedial help concerning writing problems that you might have. Students who are unable to write correctly and clearly are urged to contact the learning center for sources of remedial help.

You are responsible for keeping all graded assignments. You must present any discrepancies for a grade to be adjusted.

PLEASE NOTE: This is a work in progress. As such, if necessary, I reserve the right to modify the syllabus if needed throughout the course. (Note also that this is very rare).

Grading:

In-class participation 10 points per class (X 6 weeks) = 60
*****NOTE: PARTICIPATION definition means being ACTIVE in the discussion room at least 2 original posts and a MINIMUM of 4 responses to other students/instructor. Being ACTIVE means reading the posts of others and actively participating in adding content to the discussions.**

Court Case Analysis	25 points per case X 4 cases	100
***** See Court Case Analysis Template on next page*****		
Exam 1	=	100
Video Project	=	50
Project 1	=	90
Total Points Possible:		400

Extra Credit: Periodical Reports (maximum of 2) for 5 points each – must be less than 2 years old and must be a periodical report – not an advertisement or an encyclopedia type report or a dictionary type report. (SEE TEMPLATE ON NEXT PAGE)

COURT CASES: each individual will submit 4 court cases. No two cases can be on the same type of fraud (example, larceny, skimming, etc) See below for example.

Reading Assignments:

Week 1 June 30 – July 6: Chapter 1, 2, 3 Introduction, Skimming
Week 2 July 7 – 13: Chapter 4, 5 Cash Larceny /Check Tampering
Video Project due July 13 11:59pm
Week 3 July 14 – 20: Chapter 6, 7 Register Disb. /Billing schemes
Week 4 July 21 – 27: Chapter 8 Payroll and Expense Reimbursement
Week 5 July 28 – August 3: Chapter 9, 10 Inventory/Bribery
COURT CASES DUE by August 3 – 11:59pm
Week 6 August 4 - 11 Chapter 11, 12 Conflict of Interest/ Fraud Stmt.
Chapter 13, 14 Financial Stmt./The Big Picture

Project 2 Due August 11
Final Exam

Extra Credit:

PERIODICAL REPORTS:

The report must be from a recognized periodical – can be an online reference but NOT just any web page qualifies as a periodical. An example of a periodical is Forbes, Business Week, Big Business etc. The periodical must be no older than 2 years old. Your report should have the following information:

Your Name:
Current date:

Name of your article:
Author of the article:

Brief summary (about a paragraph or 2):

Your thoughts and analysis of the article and why you chose it: (about a paragraph or 2):

EXAMPLE COURT CASE (please use this template, make sure each section is clearly identified):

Your name: Douglas Blakemore
Current date: March 5, 2005

1. Case name, citation and court:

ZFD corp. v. John Doe
120 S.CT 1879, 2001 LEXIS 514 (2001)
U.S. Supreme Court

2. Key facts:

- A. ZFD corp. is a for-profit organization that does (what the company does)
- B. Facts about the case
- C. Etc
- D. Etc
- E. Etc (use as many bullet points as needed)

3. Issues:

Does (legal issue at stake here – may be more than one)

4. Holding:

What the court decided – guilty or not guilty

5. Courts Reasoning:

The court held that (key issues and assumptions by the court):

- A. John Doe was (or was not) X
- B. ZFD corp was (or was not) Y
- C. etc.
- D. etc.
- E. etc. (use as many points as needed)

6. YOUR Personal thoughts – Why you chose this case; what you thought about it.

SAMPLE TITLE PAGE

**Douglas L. Blakemore, Ph.D.
Ferris State University
HSCJ 317 Fraud Examination
Week 1 Assignment**

March 5, 2010

HSCJ310: Digital Forensics and Incident Response Spring Semester

Instructor:

Contact information:

Required Text: EnCase Computer Forensics: The Official EnCase Certified Examiner Study Guide (with DVD) by Steve Bunting (ISBN:0470181451)

Course Credits: 3

Course Prerequisites: HSCJ202

Course Description: Students survey the role of computer technology in digital forensics and the characteristics of an incident response plan and its implementation. Students will utilize several digital forensic tools and techniques for surveillance, gathering evidence, and reconstructing crime scenes.

Ethics Statement: The technologies, situations and implications that comprise the field of digital forensics require the highest ethical and moral standing. As such, any personal lapse of this standing – whether it is a lapse in judgment or a well constructed scheme – may constitute grounds for dismissal from the course, the program, and Ferris State University. Additionally, there is potential for legal consequence that may include prosecution. Do not duplicate or continue to access any information that may be of a criminal nature, violates privacy, and/or conflicts with this Ethics Statement. Should you come across anything of this nature don't hesitate to contact Dr. Jones immediately.

Course Policies: This syllabus is tentative in nature and may be modified by the instructor at any time. Assignments must be submitted in RTF, DOC, DOCX, or PDF format by the due date to FerrisConnect. Late work will not be accepted unless warranted by a documented emergency. No projects or course work will be accepted after 3/2/10 unless prior arrangements have been made. Grades will be posted in FerrisConnect approximately 1 week after assignments are due. There will be no grade changes after the semester ends. Submitted work may be checked using SafeAssign or similar services. If you object to having your work submitted to such services, you must notify the instructor via email no later than 1/17/10. Attendance and participation in all class meetings is required. Students missing more than 1 week of course interaction will not pass the course. Extenuating circumstances or unforeseen events will be handled at the discretion of the instructor and arrangements should be made prior to the absence. To pass this course, all assignments must be the original work of the student or team. All references and use of external sources must be appropriately documented. Plagiarism will result in not passing the course. Students must have completed at least 75% of course material and a completion contract to receive an incomplete. Any student who feels s/he may need an accommodation based on the impact of a disability should contact the instructor privately to discuss your specific needs. Cell phones should be silenced during class meetings; breaks will be provided during which calls may be made. Use of a computer for a reasons not related to course activities may result in loss of points. The Instructor reserves the right to make modifications to the course or this syllabus to accommodate unforeseen circumstances. The dates and terms in this syllabus supersede any discrepancies from any other source.

Learning Assessment Methods and Criteria: Student grades will be computed as follows:

7 Class Exercises @ 50 points each	350
5 Class quizzes @ 50 points each	250
1 Written final exam	250
1 Practical final exam	250
5 Weekly preparations @ 50 points each	250
5 weekly assignments @ 50 points each	250
7 class participations @ 10 points each	70
<hr/>	
	1670 points

NOTE: Failure to complete and submit **all** of the assignments in a timely manner will be grounds for a failing grade.

Assignments:

Weekly assignments will be discussed each week in class and due dates are noted in FerrisConnect. Assigned work is to be your own individual effort unless otherwise noted. You may use external resources, but they must be appropriately documented.

Schedule:

Reading assignments are to be completed prior to the class listed. Quiz on reading assignments will be the first agenda item each week in class. A typical class session begins with a quiz on reading material, followed by a lecture over the current week's material, followed by course activities.

Grading Scale:

A	1500 points
A-	1450
B+	1400
B	1350
B-	1300
C+	1250
C	1200
C-	1150
D	1100
F	below 1100

Course Outcomes and Assessment:**Upon completing this course, students will be able to:**

1. Identify and describe the role of computer technology in digital forensics.
 - *Assessment:* Objective testing, case study analysis, and/or project assessment.
2. Identify and describe the characteristics and implementation of an incidence response plan.
 - *Assessment:* Objective testing, case study analysis, and/or project assessment.
3. Identify and describe the capabilities of digital forensic tools.
 - *Assessment:* Objective testing, case study analysis, and/or project assessment.
4. Describe and utilize digital forensic tools for surveillance, gathering evidence and crime scene reconstruction.
 - *Assessment:* Objective testing, case study analysis, demonstration, and/or project assessment.

Course Outline including Time Allocation:

1. The role of computer technology in digital forensics. (9 hours)
 - Overview of computer technology
 - The use of computer technology in computer crime
 - Crime scene procedures
2. Incidence response plan. (12 hours)
 - Components
 - Implementation techniques and procedures
 - Utilization
3. Digital forensic tools. (12 hours)
 - Types and capabilities
 - Procedures and protocols
 - Utilization
4. Surveillance, gathering evidence, crime scene reconstruction. (12 hours)
 - Integrating digital tools into the investigation process
 - What constitutes evidence
 - Preserving evidence

Schedule

class	topics
1	hdware, fs, RAM, swap, boot, hex/bin
online reading assignments	hex/bin, data storage and file systems, first resp ch. 1, 2, 3, 4 EnCase installation
2	QUIZ, evidence aquisition
online reading assignments	EnCase new case ch 5, 6 A1: Install encase, new case, scrnshot
3	QUIZ, EnCase
online reading assignments	grep, sigs ch 7, 8 A2: file sigs
4	QUIZ, searching, sigs/hashe, ext viewers, deleted files, boot records
online reading assignments	fs and MBRVBR Ch 9 A3: search compare EnCase and FTK
5	QUIZ, searching, sigs/hashe, ext viewers, deleted files, boot records
online reading assignments	enScript ch 10 A4: deleted/overwritten
6	QUIZ, WinOS artifacts
online reading assignments	Case mgt, case closure, reports, encryption A5: mock trial analysis/prep
7	CUMULATIVE FINAL, Mock trial

ISIN 429 – Legal and Ethical Issues
Tentative Syllabus
Online
Summer, 2012 Fully ONLINE

Instructor: Doug Blakemore, Ph.D.
Contact Info: Classroom email or ismdoug@gmail.com
Phone: Google phone: 231-680-0596
SKYPE name: isidoug

Office Hours: By appointment in-person, online, by phone

Syllabus Table of Contents

Text Requirements	Page 2
Course Description	Page 2
Course Objectives	Page 2
Research and writing instructions	Page 2-4
Assignment grade points summary	Page 4
Reading assignments and due dates	Page 5
Rubric for discussion postings	Page 5-6
Periodical reports and extra credit reports instruction	Page 6
Sample title page	Page 7

PLEASE NOTE: This is a work in progress. As such, if necessary, I reserve the right to modify the syllabus if needed throughout the course. (Note also that this is very rare).

Text

Ethics in Information Technology, 3rd Edition, George W. Reynolds. Available both in print and in ebook formats

Course Description

This course is intended to investigate the legal and ethical issues in Information Security. Ethical practices, privacy, copyright and licensing issues are researched. These issues deal with proprietary and personal information, as well as electronic technologies. An understanding of current and future impact on information systems and management strategies will be explored.

Course Objectives

Upon completing this course, students will be able to:

- Understand what ethics is as it is compared to laws and morals.
- Identify and describe key issues with technology, both legal and illegal and from both the digital and physical realm.
- Identify and describe privacy concerns as it relates to technology and ethics.
- Identify and explain the role of government regulations in restricting business and personal activity
- Understand the implications of international laws in regards to digital surveillance and other online activity.

Research

When conducting research, students are strongly encouraged to make use of the Ferris Library for Information Technology and Education (FLITE) Off Campus Database Access. For more information, visit <http://library.ferris.edu/proxysetup.html>

Paper Formats

All written assignments must be in MS Word doc or docx and conform to APA style in regards to:

- having a cover page as the first page of any assignment which includes:
 - o Your name
 - o The University
 - o Class
 - o Student ID
 - o Assignment #
 - o Date

(See example later in this syllabus)

Assignments missing the title page will lose points.

- document must be **double** spaced
- document must be **LEFT** justified (never full justified)
- first lines of paragraphs are to be indented to the first tab stop.
- all uses of other people's work (including paraphrases) must be cited and referenced both in-text and end of document reference – **It is your responsibility to find out how if you don't know.**
- all assignments must be the original work of the student/team except where referenced.
- Please read Ferris State University's Academic Policy Information/Academic Honesty.

Plagiarism: Plain and simple. If you use ANYONE's work – regardless if it is a direct quote or paraphrase – then you MUST reference it. FAILURE TO REFERENCE it will result in my assuming you represented that person's work as your own and therefore stole it. Results will be failure of the work with no possible ability to make up the work. The second time in the course you are caught, it will be an automatic failure of the course.

Each student must demonstrate proficiency in the use of the English language in all work submitted for this course. Grammatical errors, spelling errors, and writing that do not express ideas clearly will affect your grade. The professor will not provide remedial help concerning writing problems that you might have. Students who are unable to write correctly and clearly are urged to contact the learning center for sources of remedial help.

You are responsible for keeping all graded assignments. You must present any discrepancies for a grade to be adjusted.

Grading

Point Summary:

Weekly discussion participation (10 points/week X 6 weeks)	=	60
Case reviews (2 per week @ 10 points each) X 6 weeks		120
***** See Template below*****		
Test 1	=	50
Test 2	=	50
Final paper	=	90
Total Points Possible:		370

Reading Assignments

Week 1 May 15 - 21:	Chapter 1, 2, Assignment for week 1 due May 21, 2012 at 11:59PM – see assignments section
Week 2 May 22 - 28:	Chapter 3 Assignment for week 2 due May 28, 2012 at 11:59PM – see assignments section
Week 3 May 29 – June 4:	Chapter 4, 5 Assignment for week 3 due June 4, 2012 at 11:59PM – see assignments section
Week 4 June 5 - 11:	Chapter 6 Assignment for week 4 due June 11, 2012 at 11:59PM – see assignments section TEST 1 DUE JUNE 11, 11:59PM
Week 5 June 12 - 18:	Chapter 7, 8 Assignment for week 5 due June 18, 2012 at 11:59PM – see assignments section
Week 6 June 19 - 26:	Chapter 9, 10 Assignment for week 6 due June 26, 2012 at 11:59PM – see assignments section Final test June 26th by 11:59 pm

DISCUSSION POSTING DETAILS:

***NOTE: PARTICIPATION definition means being ACTIVE in the discussion room. To be considered active, students must submit at least **2 original posts and a MINIMUM of 4 responses to other students/ instructor**. Being ACTIVE means reading the posts of others and actively participating in adding content to the discussions.

Discussion Posting grading rubrics:

ORIGINAL POSTS: The TWO ORIGINAL POSTINGS MUST BE SUBMITTED TO THE DISCUSSION ROOM **BEFORE FRIDAY (by 11:59pm on Thursday)** OF EACH WEEK (Weeks run from Tuesday through Monday)

RUBRIC for Original POSTINGS:

Contain a reference to outside material such as newspaper, book or web page related to the topics discussed for the week including your own personal thoughts and comments and be at least one to two paragraphs in length. The posting must be submitted by Thursday of the current week to get full credit.	Contain a reference to outside material but light on details and/or your own comments related to the current weeks topics.	Contain reference to outside material or have outside material but no/ very little personal thoughts and insights. Or no reference to outside material.	No original posting, posting is after Wednesday of the current week or posting unrelated to the current topics of the week.
3 points each maximum of 6 points (2 postings per week)	2 points each	1 point each	0 points each

RESPONSE to other students and/or the instructor's posting (**NO MORE than 2 response postings per day will be counted** – you can have 2 response postings and 1 original posting on the same day):

RUBRIC for Response POSTINGS:

Contain thoughtful response on topic and be a minimum of	Contain less than 3 sentences but still a thoughtful response	Very brief one sentence or no posting or off topic or beyond
--	---	--

3 sentences long.	on topic.	the end of the defined week dates:
1 point each (maximum of 4 points for the 4 postings)	1/2 point each	0 points each

EXTRA CREDIT: Periodical Reports (maximum of 2) for 5 points each – The article must be less than 2 years old and must be a periodical report – not an advertisement or an encyclopedia type report or a dictionary type report. Extra credit periodicals must be identified as such in the cover page and are due no later than April 29, 2012 – Post the extra credit periodicals to my classroom email address. (SEE TEMPLATE BELOW)

PERIODICAL REPORTS:

The report must be from a recognized periodical – can be an online reference but NOT just any web page qualifies as a periodical. Examples of a periodical are Forbes, Bloomberg’s Businessweek, etc. The periodical must be no older than 2 years old. Your report should have the following information:

Your Name:
Current date:

Name of your article:
Author of the article:

Brief summary (about a paragraph or 2):

Your thoughts and analysis of the article and why you chose it: (about a paragraph or 2):

SAMPLE COVER PAGE

Douglas L. Blakemore, Ph.D.
Ferris State University
HSCJ 317 Fraud Examination
Week 1 Assignment
March 5, 2010

Capstone ISIN 499
Tentative Syllabus

This syllabus is a work in progress. Every attempt will be made to maintain this syllabus throughout the course. However, from time to time changes are required to be made. The instructor reserves the right to make modifications as needed.

Instructor: Doug Blakemore, Ph.d
Contact Info: ismdoug@yahoo.com And the email in the FSUVISTA classroom
Phone: (231) 680-0596 (Google Voice #) – preferred - please note, there might be a slight delay in connecting with my phone – be patient.
Office Hours: Tuesdays from 1 – 5pm

Meeting day(s): May 19, 2012, June 23, 2012, August 4, 2012
Meeting time(s): start promptly at 9:00AM

Meeting Location: COB 310 unless other wise noted

Textbooks: None required – there will be a suggested list of books to read.

Every effort possible will be made to post grades in Ferris Connect within 1 week after assignments are due.

Course Requirements

Introduction:

This is a research paper and/or a research project. Typically the final paper is between 30 – 50 pages in length. The format of the final paper follows a 5 chapter model. Check within the online classroom for resources that will help you to put together this paper. Please be aware that this is a very significant amount of work and is a paper unlike anything you have probably ever done – or possibly even seen before.

Students need to complete the following within FerrisConnect:

- Idea Paper
- Project Proposal
- Final Project
- Program Assessment
- Project Presentation

To pass this course, all assignments must be the original work of the student. Plagiarism will result in not passing the course. Students must have completed at least 80% of course material and a completion contract to receive an incomplete. Any student who feels s/he may need an accommodation based on the impact of a disability should contact me privately to discuss your specific needs. Please contact the Disabilities Services Office, Arts and Sciences Commons, 1017k, (231) 591-3772 to coordinate reasonable accommodations for students with documented disabilities. The dates in this syllabus supersede any discrepancies from any other source.

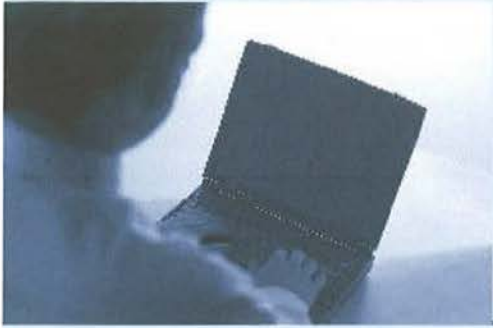
This is a different kind of paper than what almost all of you have had before. As such, it is important to keep regular contact with the instructor and submit your work to him for review periodically throughout the semester.

Also note, to pass this course and any individual assignment within the course, the assignments must be approved and graded by the instructor (Dr. Blakemore). It is not only possible but strongly encouraged to work with other instructors who have unique expertise in what you are researching, however the actual approval of all assignments and grading of papers and projects is completed by the course instructor Dr. Blakemore. Also note that you SHOULD NOT have your final paper or project copied and bound until given specific approval by Dr. Blakemore.

Grading

Scale: 92-100 = A,
90-91 = A-,
88-89 = B+,
82-87 = B,
80-81 = B-,
78-79 = C+,
72-77 = C
70-71 = C-
68-69 = D+
62-67 = D
60-61 = D-
Below 60 = F

Assignment values are listed in the Assignment section of the course.



Ferris State University

College of Business

COURSE: PROJ 350 Project Scheduling and Cost Management

INSTRUCTOR: Barbara L Ciaramitaro, PhD, PMP, CISSP, CSSLP

ONLINE INSTRUCTION : FerrisConnect

COURSE DATES: August 29 to December 9, 2011

OFFICE HOURS: IRC 222. 1:00 to 3:00 p.m. Tuesday in Big Rapids; Online Office Hours will be held weekly; Other times available by appointment.

Syllabus Changes: I reserve the right to make adjustment in this syllabus whenever I judge that the adjusted syllabus will better serve the overall learning needs of the class.

Please note that Ferris Connect Mail will be used for all course communications.

PHONE (OFFICE): (231) 591-3199 or (313) 207-6127 (preferred)

EMAIL ADDRESS: ciaramb@ferris.edu or Barbara.L.Ciaramitaro@verizon.net

FACEBOOK: Barbara L. Ciaramitaro

TWITTER: <http://twitter.com/bciaramitaro>

LINKEDIN:

<http://www.linkedin.com/in/barbaraciaramitaro>

BLOGS: <http://techademia.wordpress.com/> and <http://allthingsdigital.wordpress.com>

COURSE DESCRIPTION:

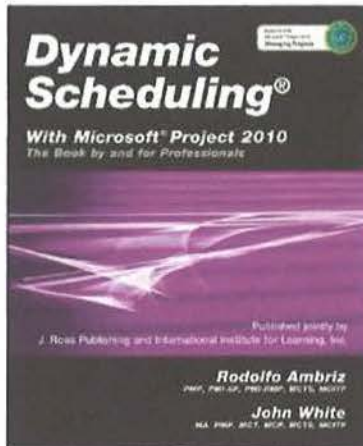
This course will build on project management fundamentals and evaluate various project management techniques used to build project schedules including time estimation, PERT, critical path, critical chain, and the use of float and buffers. This course will also examine cost estimating techniques and project budget preparation. Lastly, this course will review risk management tools and techniques including risk identification, quantitative and qualitative risk assessment, and risk mitigation strategies.

PREREQUISITES:

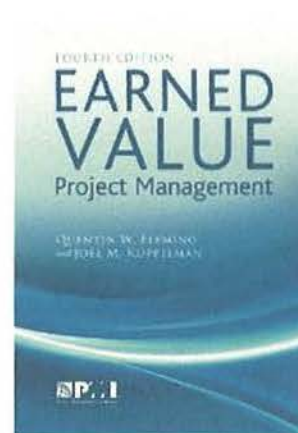
- PROJ 320 (ISYS 411)

COURSE MATERIALS:

► **TEXTBOOK(S) and SOFTWARE: REQUIRED** – Textbook Purchases through Amazon; Project 2010 through Ferris student software offering



Title:
Dynamic Scheduling with Microsoft Project 2010
Author:
Rodolfo Ambriz and John White
Publisher:
J Ross Publishing
ISBN 978-1604270617



Title:
Earned Value Project Management
Author:
Quenton Fleming and Joel Koppleman
Publisher:
Project Management Institute
ISBN: 978-1935589082

SOFTWARE



Title:
Microsoft Project 2010

▶OTHER COURSE MATERIALS:

COURSE METHODS & OBJECTIVES:

▶COURSE METHODS:

- Online Lectures and Presentations
- Discussion Forum
- Individual Assignments

▶COURSE OBJECTIVES:

- Evaluate project scheduling techniques used to build project schedules.
- Utilize project management software to

- Individual Assessments
- Midterm and Final Exams

- develop project management deliverables
- Apply scheduling techniques to activity estimation, activity precedence and resource assignments
- Use project scheduling techniques to evaluate and monitor project progress against baseline.
- Evaluate EVM (Earned Value Management) techniques.
- Apply EVM to project scheduling
- Apply EVM to project budgeting.
- Utilize EVM techniques to evaluate and monitor project progress against baseline.

ASSESSMENT GUIDELINES:

► ASSIGNMENTS:

The purpose of assignments is to reinforce the learning process. **All assignments are due Sunday of each week by 11:59 PM unless otherwise stated.**

► QUIZZES & EXAMS:

There will be weekly assignments and assessments. There will be a mid-term and final exam. The exams are cumulative. They are a combination of multiple choice and short essay questions.

For this online class, exams will be open-book and open-notes.

► DISCUSSIONS:

Students will be required to participate and interact with one another during the semester on the course discussion boards. Discussion questions will be posted on a weekly basis. You are required to create at least one original reply to the discussion topic and respond to at least two of your classmates for each discussion question posted. Early posting in the Discussion will ensure you receive replies from fellow students. Your weekly discussion posting will be graded using the following grading rubric.

Discussion Questions Grading Rubric

Points	Description
--------	-------------

15 points	Responded to all questions with interaction among other students. Responses began early and were often. Responses were thoughtful and topical. Outside sources, previous knowledge, and real life experience were used in responses. The flow and direction of the discussion was greatly affected by contribution.
10-14 points	Did not respond directly to all questions, and/or did not respond to others with comments or questions and/or all responses are made in one visit to the site. Responses lacked deep analysis or thought..
9 or less points	Minimal participation. Did not respond to all posted questions. All responses are made in one visit to the site. Responses lacked analysis or thoughtfulness (applied text or lecture teaching points or real life examples) and/or was not topical (related to the text and lectures.)
0	No participation. No response

►MAKE-UP POLICY:

There will be no make up quizzes, exams, assignments or discussion question postings. It may be possible to pre-schedule a quiz or exam but students must contact the instructor directly and this will be determined on an individual basis.

COURSE POINTS & GRADING SCALE:

►COURSE POINTS:

►GRADING SCALE:

Your performance in this course will be assessed as follows:

950 and above = A
 890 - 949 = A-
 850 - 889 = B+
 820 - 849 = B
 780 - 819 = B-
 750 - 779 = C+
 700 - 749 = C
 650 - 699 = C-
 600 - 649 = D+
 550 - 599 = D
 below 550 = F

Assessment	Points
Mid-Term and Final Exam (142.5 pts) =	285
Individual Assignments (13 @ 20 pts each)=	260
Individual Assessments (13 @ 20 points each)	260
Discussion Board (13 @ 15 Points each) =	195
Total Pointes	1000

ASSIGNMENT SCHEDULE:

WEEK BEGINS	DUE	THIS WEEK'S TOPICS	ASSIGNED THIS WEEK
1		• Course Introduction	• Read

8/29/11		<ul style="list-style-type: none"> • Introduction to Microsoft Project 2010 	<p>Dynamic Scheduling – Chapters 1 and 2</p> <ul style="list-style-type: none"> • Week #1 Discussion Board • Individual Assignment 1 • Individual Assessment 1
2 9/5/11	<ul style="list-style-type: none"> • Week #1 Discussion Board • Individual Assignment 1 • Individual Assessment 1 • Due no later than 11:59 pm on Sunday, 9/4/11 	<ul style="list-style-type: none"> • Creating your Work Breakdown Structure • The Art of Estimating 	<ul style="list-style-type: none"> • Read Dynamic Scheduling – Chapters 3 and 4 • Individual Assignment 2 • Individual Assessment 2
3 9/12/11	<ul style="list-style-type: none"> • Week #2 Discussion Board • Individual Assignment 2 • Individual Assessment 2 • Due no later than 11:59 pm on Sunday, 9/11/11 	<ul style="list-style-type: none"> • Understanding Task Dependencies, Deadlines and Constraints 	<ul style="list-style-type: none"> • Read Dynamic Scheduling – Chapters 5 and 6 • Week #3 Discussion Board • Individual Assignment 3 • Individual Assessment 3
4 9/19/11	<ul style="list-style-type: none"> • Week #3 Discussion Board • Individual Assignment 3 • Individual Assessment 3 • Due no later than 11:59 pm on Sunday, 9/18/11 	<ul style="list-style-type: none"> • Identifying Project Resources • Assigning Roles and Responsibilities 	<ul style="list-style-type: none"> • Read Dynamic Scheduling – Chapters 7 and 8 • Week #4 Discussion Board • Individual Assignment 4

			<ul style="list-style-type: none"> Individual Assessment 4
<p>5 9/26/11</p>	<ul style="list-style-type: none"> Week #4 Discussion Board Individual Assignment 4 Individual Assessment 4 Due no later than 11:59 pm on Sunday, 9/25/11 	<ul style="list-style-type: none"> Optimizing and Maintaining the Project Schedule Project Reporting 	<ul style="list-style-type: none"> Read Dynamic Scheduling – Chapters 9 to 11 Week #5 Discussion Board Individual Assignment 5 Individual Assessment 5
<p>6 10/3/11</p>	<ul style="list-style-type: none"> Week #5 Discussion Board Individual Assignment 5 Individual Assessment 5 Due no later than 11:59 pm on Sunday, 10/1/11 	<ul style="list-style-type: none"> Introduction to EVM (Earned Value Management) Evaluating the Project 	<ul style="list-style-type: none"> Read Dynamic Scheduling – Chapters 13 and 14 Week #5 Discussion Board Individual Assignment 6 Individual Assessment 6
<p>7 10/10/11</p>	<ul style="list-style-type: none"> Week #6 Discussion Board Individual Assignment 6 Individual Assessment 6 Due no later than 11:59 pm on Sunday, 10/9/11 	<ul style="list-style-type: none"> Project Scheduling Review 	<ul style="list-style-type: none"> Mid Term
<p>8 10/17/11</p>	<ul style="list-style-type: none"> Mid-Term Due no later than 11:59 pm on Sunday, 10/16/11 	<ul style="list-style-type: none"> Overview of Earned Value Project Management 	<ul style="list-style-type: none"> Read Earned Value – Chapters 1 to 3

			<ul style="list-style-type: none"> • Week #8 Discussion Board • Individual Assignment 7 • Individual Assessment 7
<p>9 10/24/11</p>	<ul style="list-style-type: none"> • Week #8 Discussion Board • Individual Assignment 7 • Individual Assessment 7 • Due no later than 11:59 pm on Sunday, 10/23/11 	<ul style="list-style-type: none"> • Overview of Earned Value Project Management 	<ul style="list-style-type: none"> • Read Earned Value – Chapters 4 to 5 • Week #9 Discussion Board • Individual Assignment 8 • Individual Assessment 8
<p>10 10/31/11</p>	<ul style="list-style-type: none"> • Week #9 Discussion Board • Individual Assignment 8 • Individual Assessment 8 • Due no later than 11:59 pm on Sunday, 10/30/11 	<ul style="list-style-type: none"> • Planning and Scheduling the Project • Establish Project Budget 	<ul style="list-style-type: none"> • Read Earned Value – Chapters 6 to 8 • Week #10 Discussion Board • Individual Assignment 9 • Individual Assessment 9
<p>11 11/7/11</p>	<ul style="list-style-type: none"> • Week #10 Discussion Board • Individual Assignment 9 • Individual Assessment 9 • Due no later than 11:59 pm on Sunday, 11/16/11 	<ul style="list-style-type: none"> • Establish EVM Baseline • Apply EVM to Procurement 	<ul style="list-style-type: none"> • Read Earned Value – Chapters 9 to 10 • Week #11 Discussion Board • Individual Assignment 10

			<ul style="list-style-type: none"> Individual Assessment 10
12 11/14/11	<ul style="list-style-type: none"> Week #11 Discussion Board Individual Assignment 10 Individual Assessment 10 Due no later than 11:59 pm on Sunday, 11/13/11 	<ul style="list-style-type: none"> Monitor Performance against EVM Baseline Forecasting Final Cost 	<ul style="list-style-type: none"> Read Earned Value – Chapters 11 to 12 Week #12 Discussion Board Individual Assignment 11 Individual Assessment 11
13 11/21/11	<ul style="list-style-type: none"> Week #12 Discussion Board Individual Assignment 11 Individual Assessment 11 Due no later than 11:59 pm on Sunday, 11/20/11 	<ul style="list-style-type: none"> Portfolio Project Management with EVM 	<ul style="list-style-type: none"> Read Earned Value – Chapters 13 to 14 Week #13 Discussion Board Individual Assignment 12 Individual Assessment 12
14 11/28/11	<ul style="list-style-type: none"> Week #13 Discussion Board Individual Assignment 12 Individual Assessment 12 Due no later than 11:59 pm on Sunday, 11/27/11 	<ul style="list-style-type: none"> EVM and Sarbanes Oxley 	<ul style="list-style-type: none"> Read Earned Value – Chapter 15 Week #14 Discussion Board Individual Assignment 13 Individual Assessment 13
15 12/5/11	<ul style="list-style-type: none"> Week #14 Discussion Board Individual Assignment 13 Individual Assessment 13 	<ul style="list-style-type: none"> Course Review 	

	<ul style="list-style-type: none"> • Due no later than 11:59 pm on Sunday, 12/4/11 		
16 12/9/11	<ul style="list-style-type: none"> • Final Exam Due • Due no later than 11:59 pm on Friday, 12/16/11 	<ul style="list-style-type: none"> • Final Exam 	

STATEMENT REGARDING PROFESSIONAL CONDUCT

Ferris students are expected to conduct themselves in a manner that is conducive to continued growth toward a business and/or professional career. Each student is expected to attend classes regularly and to be fully prepared. All students are expected to act professionally and with a high degree of ethical conduct while applying themselves fully to the job of learning. All communications are expected to be conducted in a professional manner, whether written or oral.

It is the student's obligation to know and observe all University policies and procedures and to keep current by reading the materials posted on the Ferris University Web Site and in its printed policies and bulletins.

STATEMENT REGARDING ACADEMIC MISCONDUCT

Plagiarism, unauthorized collusion on examinations, theft, sale, purchase or other unauthorized procurement of examinations or essay material, use of unauthorized aids while taking an examination, having someone else take an exam in your place or submitting for credit any paper not written by student, taking an exam for another student, copying of "do not copy" designated library materials, copying copyrighted software and destruction of equipment by introducing a computer virus and other similar actions are considered to be academic misconduct and unacceptable for students enrolled at Ferris State University.

STATEMENT REGARDING DIVERSITY

This course embraces the Ferris Core Values of diversity by providing an environment which is supportive, safe and welcoming. We will listen respectfully to a diversity of ideas, beliefs and cultures presented by the members of the class.

Core Values

- **Collaboration:** Ferris contributes to the advancement of society by building partnerships with students, alumni, business and industry, government bodies, accrediting agencies, and the communities the University serves.

- **Diversity:** By providing a campus which is supportive, safe, and welcoming, Ferris embraces a diversity of ideas, beliefs, and cultures.
- **Ethical Community:** Ferris recognizes the inherent dignity of each member of the University community and treats everyone with respect. Our actions are guided by fairness, honesty, and integrity.
- **Excellence:** Committed to innovation and creativity, Ferris strives to produce the highest quality outcomes in all its endeavors.
- **Learning:** Ferris State University values education that is career-oriented, balances theory and practice, develops critical thinking, emphasizes active learning, and fosters responsibility and the desire for the lifelong pursuit of knowledge.
- **Opportunity:** Ferris, with a focus on developing career skills and knowledge, provides opportunities for civic engagement, leadership development, advancement, and success.

COB Syllabus Attachment is posted separately.



Ferris State University

College of Business

COURSE: PROJ 351 Project Communication and Risk Management

INSTRUCTOR: Barbara L Ciaramitaro, PhD,
PMP, CISSP, CSSLP

ONLINE INSTRUCTION : FerrisConnect
COURSE DATES: August 29 to December 9,
2011

OFFICE HOURS: 1:00 to 3:00 p.m. Tuesday in
Big Rapids; Online Office Hours will be held
weekly; Other times available by appointment.

Syllabus Changes: I reserve the right to make
adjustment in this syllabus whenever I judge that
the adjusted syllabus will better serve the overall
learning needs of the class.

**Please note that Ferris Connect Mail will be
used for all course communications.**

PHONE (OFFICE): (231) 591-3199 or (313) 207-
6127 (preferred)

EMAIL ADDRESS: ciaramb@ferris.edu or
Barbara.L.Ciaramitaro@verizon.net

FACEBOOK: Barbara L. Ciaramitaro

TWITTER: <http://twitter.com/bciaramitaro>

LINKEDIN:

<http://www.linkedin.com/in/barbaraciaramitaro>

BLOGS: <http://techademia.wordpress.com/> and
<http://allthingsdigital.wordpress.com>

COURSE DESCRIPTION:

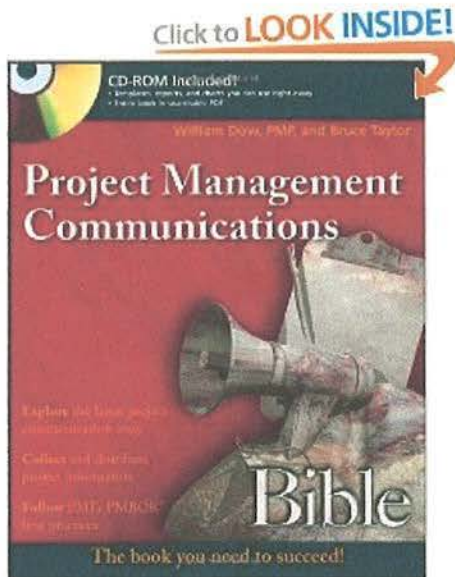
Communication activities are estimated to take up to 90% of a project manager's time. This course will take an in depth look at project communication management, team building and conflict management. Ethical issues, professional responsibility and diversity issues related to project management will be discussed. The course will examine various communication and conflict resolution techniques; the challenges of managing project teams particularly in the virtual environment; and assess various team building tools and techniques. This course will also review risk management tools and techniques including risk identification, quantitative and qualitative risk assessment, and risk mitigation strategies.

PREREQUISITES:

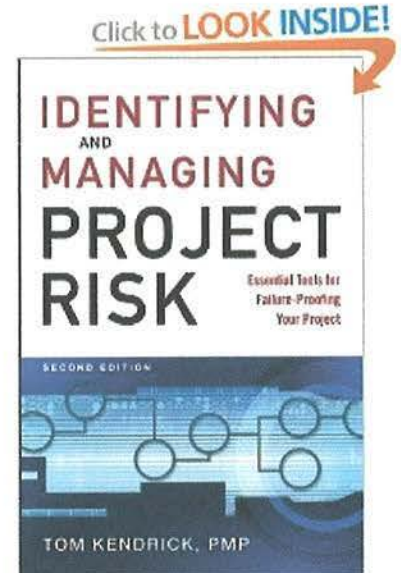
- PROJ 320

COURSE MATERIALS:

►TEXTBOOK(S): REQUIRED Textbook Available through Amazon



Title: Project Management: Communications
Author: William Dow and Bruce Taylor
Publisher: Wiley
ISBN 978-0470137406



►OTHER COURSE MATERIALS:

COURSE METHODS & OBJECTIVES:

►COURSE METHODS:

- Online Lectures and Presentations
- Discussion Forum
- Individual Assignments
- Individual Assessments
- Midterm and Final Exams

►COURSE OBJECTIVES:

- Construct and/or describe Communication Plans, Information Distribution methodologies, Stakeholder Expectation Management, and Performance Reports.
- Evaluate the effectiveness of various conflict resolution techniques
- Distinguish social, cultural, diversity, and distance issues related to the management of traditional and virtual teams.
- Develop team building plans and communicate ethical standards and

requirements.

- Distinguish the various steps involved in risk management from risk identification, through risk assessment, risk mitigation and the development of a risk contingency budget.
- Compare and contrast quantitative and qualitative risk analysis.

ASSESSMENT GUIDELINES:

► ASSIGNMENTS:

The purpose of assignments is to reinforce the learning process. **All assignments are due Sunday of each week by 11:59 PM unless otherwise stated.**

► QUIZZES & EXAMS:

There will be weekly assignments and assessments. There will be a mid-term and final exam. The exams are cumulative. They are a combination of multiple choice and short essay questions.

For this online class, exams will be open-book and open-notes.

► DISCUSSIONS:

Students will be required to participate and interact with one another during the semester on the course discussion boards. Discussion questions will be posted on a weekly basis. You are required to create at least one original reply to the discussion topic and respond to at least two of your classmates for each discussion question posted. Early posting in the Discussion will ensure you receive replies from fellow students. Your weekly discussion posting will be graded using the following grading rubric.

Discussion Questions Grading Rubric

Points	Description
15 points	Responded to all questions with interaction among other students. Responses began early and were often. Responses were thoughtful and topical. Outside sources, previous knowledge, and real life experience were used in responses. The flow and direction of the discussion was greatly affected by contribution.

10-14 points	Did not respond directly to all questions, and/or did not respond to others with comments or questions and/or all responses are made in one visit to the site. Responses lacked deep analysis or thought..
9 or less points	Minimal participation. Did not respond to all posted questions. All responses are made in one visit to the site. Responses lacked analysis or thoughtfulness (applied text or lecture teaching points or real life examples) and/or was not topical (related to the text and lectures.)
0	No participation. No response

►MAKE-UP POLICY:

There will be no make up quizzes, exams, assignments or discussion question postings. It may be possible to pre-schedule a quiz or exam but students must contact the instructor directly and this will be determined on an individual basis.

COURSE POINTS & GRADING SCALE:

►COURSE POINTS:

►GRADING SCALE:

Your performance in this course will be assessed as follows:

- 950 and above = A
- 890 - 949 = A-
- 850 - 889 = B+
- 820 - 849 = B
- 780 - 819 = B-
- 750 - 779 = C+
- 700 - 749 = C
- 650 - 699 = C-
- 600 - 649 = D+
- 550 - 599 = D
- below 550 = F

Assessment	Points
Mid-Term and Final Exam (142.5 pts) =	285
Individual Assignments (13 @ 20 pts each)=	260
Individual Assessments (13 @ 20 points each)	260
Discussion Board (13 @ 15 Points each) =	195
Total Points	1000

ASSIGNMENT SCHEDULE:

WEEK BEGINS	DUE	THIS WEEK'S TOPICS	ASSIGNED THIS WEEK
1 8/29/11		<ul style="list-style-type: none"> • Course Introduction • Introduction to Project Management Communications • Planning Project 	<ul style="list-style-type: none"> • Read Project Management Communications – Chapters 1 to 3

		Communications	<ul style="list-style-type: none"> • Week #1 Discussion Board • Individual Assignment 1 • Individual Assessment 1
2 9/5/11	<ul style="list-style-type: none"> • Week #1 Discussion Board • Individual Assignment 1 • Individual Assessment 1 • Due no later than 11:59 pm on Sunday, 9/4/11 	<ul style="list-style-type: none"> • Using Project Communications in the Project Integration, Scope and Time Knowledge Areas 	<ul style="list-style-type: none"> • Read Project Management Communications – Chapters 4 to 6 • Week # 2 Discussion Board • Individual Assignment 2 • Individual Assessment 2
3 9/12/11	<ul style="list-style-type: none"> • Week #2 Discussion Board • Individual Assignment 2 • Individual Assessment 2 • Due no later than 11:59 pm on Sunday, 9/11/11 	<ul style="list-style-type: none"> • Using Project Communications in the Project Cost, Quality and Human Resource Knowledge Areas 	<ul style="list-style-type: none"> • Read Project Management Communications – Chapters 7 to 9 • Week #3 Discussion Board • Individual Assignment 3 • Individual Assessment 3
4 9/19/11	<ul style="list-style-type: none"> • Week #3 Discussion Board • Individual Assignment 3 • Individual Assessment 3 • Due no later than 11:59 pm on Sunday, 9/18/11 	<ul style="list-style-type: none"> • Using Project Communications in the Project Communication Knowledge Area 	<ul style="list-style-type: none"> • Read Project Management Communications – Chapters 10 to 11 • Week #4 Discussion Board • Individual Assignment 4 • Individual Assessment 4
5 9/26/11	<ul style="list-style-type: none"> • Week #4 Discussion Board 	<ul style="list-style-type: none"> • Using Project Communications in the Project Risk and 	<ul style="list-style-type: none"> • Read Project Management Communicati

	<ul style="list-style-type: none"> • Individual Assignment 4 • Individual Assessment 4 • Due no later than 11:59 pm on Sunday, 9/25/11 	Procurement Knowledge Areas	<ul style="list-style-type: none"> • ons – Chapters 12 to 13 • Week #5 Discussion Board • Individual Assignment 5 • Individual Assessment 5
6 10/3/11	<ul style="list-style-type: none"> • Week #5 Discussion Board • Individual Assignment 5 • Individual Assessment 5 • Due no later than 11:59 pm on Sunday, 10/1/11 	<ul style="list-style-type: none"> • Using Project Communications in the Project Life Cycle Phases of Initiation and Planning 	<ul style="list-style-type: none"> • Read Project Management Communications – Chapters 14 to 17 • Week #5 Discussion Board • Individual Assignment 6 • Individual Assessment 6
7 10/10/11	<ul style="list-style-type: none"> • Week #6 Discussion Board • Individual Assignment 6 • Individual Assessment 6 • Due no later than 11:59 pm on Sunday, 10/9/11 	<ul style="list-style-type: none"> • Using Project Communications in the Project Life Cycle Phases of Executing 	<ul style="list-style-type: none"> • Read Project Management Communications – Chapters 18 to 19 • Week #5 Discussion Board • Individual Assignment 7 • Individual Assessment 7
8 10/17/11	<ul style="list-style-type: none"> • Week #7 Discussion Board • Individual Assignment 7 • Individual Assessment 7 • Due no later than 11:59 pm on Sunday, 10/16/11 	<ul style="list-style-type: none"> • Using Project Communications in the Project Life Cycle Phases of Monitoring and Closing 	<ul style="list-style-type: none"> • Read Project Management Communications – Chapters 20 to 21 • Week #8 Discussion Board • Individual Assignment 8 • Individual

			Assessment 8
9 10/24/11	<ul style="list-style-type: none"> • Week #8 Discussion Board • Individual Assignment 8 • Individual Assessment 8 • Due no later than 11:59 pm on Sunday, 10/23/11 	<ul style="list-style-type: none"> • Introduction to Risk Management • Mid-Term 	<ul style="list-style-type: none"> • Read Identifying and Managing Project Risk – Chapters 1 and 2 • Mid-term
10 10/31/11	<ul style="list-style-type: none"> • Mid-Term Exam • Due no later than 11:59 pm on Sunday, 10/30/11 	<ul style="list-style-type: none"> • Identifying Project Scope, Schedule and Resource Risk 	<ul style="list-style-type: none"> • Read Identifying and Managing Project Risk – Chapters 3 to 5 • Week #10 Discussion Board • Individual Assignment 9 • Individual Assessment 9
11 11/7/11	<ul style="list-style-type: none"> • Week #10 Discussion Board • Individual Assignment 9 • Individual Assessment 9 • Due no later than 11:59 pm on Sunday, 11/16/11 	<ul style="list-style-type: none"> • Assessing and Managing Activity Risks 	<ul style="list-style-type: none"> • Read Identifying and Managing Project Risk – Chapters 6 to 8 • Week #11 Discussion Board • Individual Assignment 10 • Individual Assessment 10
12 11/14/11	<ul style="list-style-type: none"> • Week #11 Discussion Board • Individual Assignment 10 	<ul style="list-style-type: none"> • Assessing and Managing Project Risks 	<ul style="list-style-type: none"> • Read Identifying and Managing Project Risk

	<ul style="list-style-type: none"> • Individual Assessment 10 • Due no later than 11:59 pm on Sunday, 11/13/11 • 		<ul style="list-style-type: none"> – Chapters 9 to 10 • Week #12 Discussion Board • Individual Assignment 11 • Individual Assessment 11
13 11/21/11	<ul style="list-style-type: none"> • Week #12 Discussion Board • Individual Assignment 11 • Individual Assessment 11 • Due no later than 11:59 pm on Sunday, 11/20/11 	<ul style="list-style-type: none"> • Monitoring and Controlling Risks • Risks in the Closing Phase 	<ul style="list-style-type: none"> • Read Identifying and Managing Project Risk – Chapters 11 to 12 • Week #13 Discussion Board • Individual Assignment 12 • Individual Assessment 12
14 11/28/11	<ul style="list-style-type: none"> • Week #13 Discussion Board • Individual Assignment 12 • Individual Assessment 12 • Due no later than 11:59 pm on Sunday, 11/27/11 	<ul style="list-style-type: none"> • Enterprise Project Risk Management 	<ul style="list-style-type: none"> • Read Identifying and Managing Project Risk – Chapters 13 to 14 • Week #14 Discussion Board • Individual Assignment 13 • Individual Assessment 13
15 12/5/11	<ul style="list-style-type: none"> • Week #14 Discussion Board • Individual Assignment 13 • Individual Assessment 13 	<ul style="list-style-type: none"> • Final Exam 	<ul style="list-style-type: none"> • Final Exam

	<ul style="list-style-type: none"> • Due no later than 11:59 pm on Sunday, 12/4/11 		
12/9/11	<ul style="list-style-type: none"> • Final Exam Due • Due no later than 11:59 pm on Friday, 12/9/11 		

STATEMENT REGARDING PROFESSIONAL CONDUCT

Ferris students are expected to conduct themselves in a manner that is conducive to continued growth toward a business and/or professional career. Each student is expected to attend classes regularly and to be fully prepared. All students are expected to act professionally and with a high degree of ethical conduct while applying themselves fully to the job of learning. All communications are expected to be conducted in a professional manner, whether written or oral.

It is the student's obligation to know and observe all University policies and procedures and to keep current by reading the materials posted on the Ferris University Web Site and in its printed policies and bulletins.

STATEMENT REGARDING ACADEMIC MISCONDUCT

Plagiarism, unauthorized collusion on examinations, theft, sale, purchase or other unauthorized procurement of examinations or essay material, use of unauthorized aids while taking an examination, having someone else take an exam in your place or submitting for credit any paper not written by student, taking an exam for another student, copying of "do not copy" designated library materials, copying copyrighted software and destruction of equipment by introducing a computer virus and other similar actions are considered to be academic misconduct and unacceptable for students enrolled at Ferris State University.

STATEMENT REGARDING DIVERSITY

This course embraces the Ferris Core Values of diversity by providing an environment which is supportive, safe and welcoming. We will listen respectfully to a diversity of ideas, beliefs and cultures presented by the members of the class.

Core Values

- **Collaboration:** Ferris contributes to the advancement of society by building partnerships with students, alumni, business and industry, government bodies, accrediting agencies, and the communities the University serves.

- **Diversity:** By providing a campus which is supportive, safe, and welcoming, Ferris embraces a diversity of ideas, beliefs, and cultures.
- **Ethical Community:** Ferris recognizes the inherent dignity of each member of the University community and treats everyone with respect. Our actions are guided by fairness, honesty, and integrity.
- **Excellence:** Committed to innovation and creativity, Ferris strives to produce the highest quality outcomes in all its endeavors.
- **Learning:** Ferris State University values education that is career-oriented, balances theory and practice, develops critical thinking, emphasizes active learning, and fosters responsibility and the desire for the lifelong pursuit of knowledge.
- **Opportunity:** Ferris, with a focus on developing career skills and knowledge, provides opportunities for civic engagement, leadership development, advancement, and success.

COB Syllabus Attachment is posted separately.



College of Business

PROJ 420 – Project Procurement and Certification Preparation

INSTRUCTOR: Barbara L Ciaramitaro, PhD,
PMP, CISSP, CSSLP

ONLINE INSTRUCTION : FerrisConnect
COURSE DATES: May 15 to August 8, 2012

OFFICE HOURS: Available by appointment.

Syllabus Changes: I reserve the right to make adjustment in this syllabus whenever I judge that the adjusted syllabus will better serve the overall learning needs of the class.

Please note that Ferris Connect Mail will be used for all course communications.

PHONE (OFFICE): (231) 591-3199 or (313) 207-6127 (preferred)

EMAIL ADDRESS: ciaramb@ferris.edu or Barbara.L.Ciaramitaro@verizon.net

FACEBOOK: Barbara L. Ciaramitaro

TWITTER: <http://twitter.com/bciaramitaro>

LINKEDIN:

<http://www.linkedin.com/in/barbaraciaramitaro>

BLOGS: <http://techademia.wordpress.com/> and <http://allthingsdigital.wordpress.com>

COURSE DESCRIPTION:

Course Description: This course will examine the various challenges present in the procurement process including the bid process, vendor selection and contract management. This course will provide best practices, tools and techniques to manage procurement through its entire process from Bid Document Preparation to

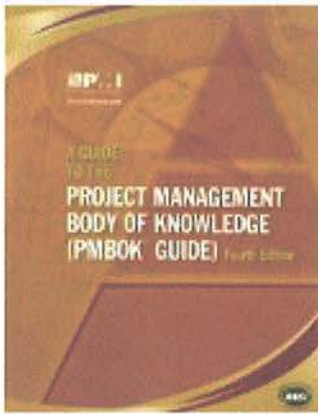
Contract Closure. This course will also review of the Project Management Body of Knowledge in terms of preparing for the PMP and CAPM Certification tests.

PREREQUISITES:

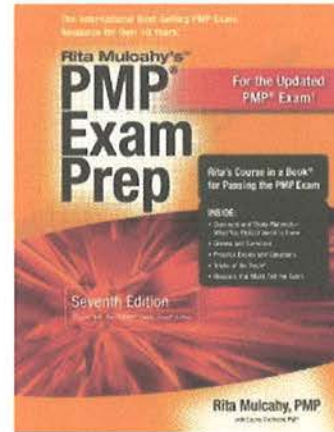
- None

COURSE MATERIALS:

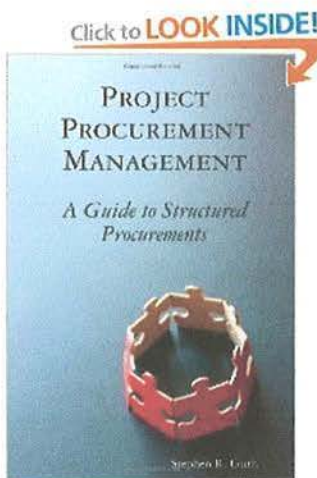
► **TEXTBOOK(S): REQUIRED**



Title:
Project Management Body of Knowledge (PMBOK)
Author: PMI
Publisher: PMI
ISBN 978-1933890517



Title: PMP Exam Prep
Author: Rita Mulcahey
Publisher: RMC Publications
ISBN: 978-1932735413



Title:
Project Procurement Management
Author: Stephen Guth
Publisher: Lulu
ISBN: 978-0557209033

▶OTHER COURSE MATERIALS:

COURSE METHODS & OBJECTIVES:

▶COURSE METHODS:

- Online Lectures and Presentations
- Discussion Forum
- Individual Assignments
- Individual Assessments
- Sample Certification Exams

▶COURSE OBJECTIVES:

1. Evaluate various bid documents and their suitability to different purchase and vendor requirements.
 - Assessment: Given scenarios, students will construct various bid documents and document their applicability to different procurement requirements.

2. Evaluate vendor selection criteria based on the project and product requirements.
 - Assessment: Classroom exercises, case studies, assignments and/or assessments
3. Examine legal criteria for procurement management including contract administration and contract closure.
 - Assessment: Given a scenario or problem set, students will determine legal requirements.
4. Distinguish social, cultural, diversity, and distance issues related to procurement managements.
 - Assessment: Classroom exercises, case studies, assignments and/or assessments.
5. Develop procurement management plans and integrate ethical and professional responsibility standards.
 - Assessment: Classroom exercises, case studies, assignments and/or assessments.
6. Review the Project Management Body of Knowledge in preparation for the PMP and C APM certification tests.
 - Assessment: Review questions, classroom exercise

ASSESSMENT GUIDELINES:

▶ ASSIGNMENTS:

The purpose of assignments is to reinforce the learning process. **All assignments are due Sunday of each week by 11:59 PM unless otherwise stated.**

▶ QUIZZES & EXAMS:

There will be a mid-term and final exam. The exams are cumulative. They are a combination of multiple choice and short essay questions.

For this online class, exams will be open-book and open-notes.

►DISCUSSIONS:

Students will be required to participate and interact with one another during the semester on the course discussion boards. Discussion questions will be posted on a weekly basis. You are required to create at least one original reply to the discussion topic and respond to at least two of your classmates for each discussion question posted. Early posting in the Discussion will ensure you receive replies from fellow students. Your weekly discussion posting will be graded using the following grading rubric.

Discussion Questions Grading Rubric

Points	Description
15 points	Responded to all questions with interaction among other students. Responses began early and were often. Responses were thoughtful and topical. Outside sources, previous knowledge, and real life experience were used in responses. The flow and direction of the discussion was greatly affected by contribution.
10-14 points	Did not respond directly to all questions, and/or did not respond to others with comments or questions and/or all responses are made in one visit to the site. Responses lacked deep analysis or thought..
9 or less points	Minimal participation. Did not respond to all posted questions. All responses are made in one visit to the site. Responses lacked analysis or thoughtfulness (applied text or lecture teaching points or real life examples) and/or was not topical (related to the text and lectures.)
0	No participation. No response

►MAKE-UP POLICY:

There will be no make up quizzes, exams, assignments or discussion question postings. It may be possible to pre-schedule a quiz or exam but students must contact the instructor directly and this will be determined on an individual basis.

COURSE POINTS & GRADING SCALE:

►COURSE POINTS:

Your performance in this course will be assessed as follows:

Assessment	Points
Mid-Term and Final Exams (200 pts) =	400
Individual Assignments (11 @ 30 pts	300

►GRADING SCALE:

950 and above = A
890 - 949 = A-
850 - 889 = B+
820 - 849 = B
780 - 819 = B-
750 - 779 = C+

each)=	
Individual Assessments (11@ 30 points each)	300
Total Points	1000

700 - 749 = C
650 - 699 = C-
600 - 649 = D+
550 - 599 = D
below 550 = F

CLASS SCHEDULE:

WEEK BEGINS	DUE	THIS WEEK'S TOPICS	ASSIGNED THIS WEEK
1 5/15/12		<ul style="list-style-type: none"> • Introduction to Project Management and the Project Management Process Groups • Introduction to Project Management Knowledge Areas 	<ul style="list-style-type: none"> • Read PMBOK – Sections 1, 2, and 3 • Review PMP Exam Prep – Chapters 1, 2, and 3 • Individual Assignment 1 • Individual Assessment 1
2 5/21/12	<ul style="list-style-type: none"> • Individual Assignment 1 • Individual Assessment 1 • Due no later than 11:59 pm on Sunday, 5/20/12 	<ul style="list-style-type: none"> • Project Integration Management 	<ul style="list-style-type: none"> • Read PMBOK – Section 4 • Review PMP Exam Prep – Chapter 4 • Individual Assignment 2 • Individual Assessment 2
3 5/28/12	<ul style="list-style-type: none"> • Individual Assignment 2 • Individual Assessment 2 • Due no later than 11:59 pm on Sunday, 5/27/12 	<ul style="list-style-type: none"> • Project Scope Management 	<ul style="list-style-type: none"> • Read PMBOK – Section 5 • Review PMP Exam Prep – Chapter 5 • Individual Assignment 3 • Individual

			Assessment 3
4 6/4/12	<ul style="list-style-type: none"> • Individual Assignment 3 • Individual Assessment 3 • Due no later than 11:59 pm on Sunday, 6/3/12 	<ul style="list-style-type: none"> • Project Time Management 	<ul style="list-style-type: none"> • Read PMBOK – Section 6 • Review PMP Exam Prep – Chapter 6 • Individual Assignment 4 • Individual Assessment 4
5 6/11/12	<ul style="list-style-type: none"> • Individual Assignment 4 • Individual Assessment 4 • Due no later than 11:59 pm on Sunday, 6/10/12 	<ul style="list-style-type: none"> • Project Cost Management 	<ul style="list-style-type: none"> • Read PMBOK – Section 7 • Review PMP Exam Prep – Chapter 7 • Individual Assignment 5 • Individual Assessment 5
6 6/18/12	<ul style="list-style-type: none"> • Individual Assignment 5 • Individual Assessment 5 • Due no later than 11:59 pm on Sunday, 6/17/12 	<ul style="list-style-type: none"> • Project Quality Management 	<ul style="list-style-type: none"> • Read PMBOK – Section 8 • Review PMP Exam Prep – Chapter 8 • Individual Assignment 6 • Individual Assessment 6 • Mid-Term Examination
7 6/27/12	<ul style="list-style-type: none"> • Mid-Term Examination • Individual Assignment 6 • Individual Assessment 6 • Due no later than 11:59 pm on Sunday, 	<ul style="list-style-type: none"> • Project Human Resource Management 	<ul style="list-style-type: none"> • Read PMBOK – Section 9 • Review PMP Exam Prep – Chapter 9 • Individual Assignment 7

	6/26/12		<ul style="list-style-type: none"> Individual Assessment 7
8 7/2/12	<ul style="list-style-type: none"> Individual Assignment 7 Individual Assessment 7 Due no later than 11:59 pm on Sunday, 7/1/12 	<ul style="list-style-type: none"> Project Communications Management 	<ul style="list-style-type: none"> Read PMBOK – Section 10 Review PMP Exam Prep – Chapter 10 Individual Assignment 7 Individual Assessment 7
9 7/9/12	<ul style="list-style-type: none"> Week #8 Discussion Board Individual Assignment 7 Individual Assessment 7 Due no later than 11:59 pm on Sunday, 7/8/12 	<ul style="list-style-type: none"> Project Risk Management 	<ul style="list-style-type: none"> Read PMBOK – Section 11 Review PMP Exam Prep – Chapter 11 Read Project Procurement Management pages 1-94 Individual Assignment 8 Individual Assessment 8
10 7/15/12	<ul style="list-style-type: none"> Week #9 Discussion Board Individual Assignment 8 Individual Assessment 8 Due no later than 11:59 pm on Sunday, 7/14/12 	<ul style="list-style-type: none"> Project Procurement Management 	<ul style="list-style-type: none"> Read PMBOK – Section 12 Review PMP Exam Prep – Chapter 13 Read Project Procurement Management pages 95-152

			<ul style="list-style-type: none"> • Read Project • Individual Assignment 9 • Individual Assessment 9
11 7/22/12	<ul style="list-style-type: none"> • Week #10 Discussion Board • Individual Assignment 9 • Individual Assessment 9 • Due no later than 11:59 pm on Sunday, 7/21/12 	<ul style="list-style-type: none"> ○ Project Procurement Management 	<ul style="list-style-type: none"> • Read Project Procurement Management pages 153-196 • Review PMP Exam Prep – Chapter 13 • Individual Assignment 10 • Individual Assessment 10
12 7/30/12	<ul style="list-style-type: none"> • Week #11 Discussion Board • Individual Assignment 10 • Individual Assessment 10 • Due no later than 11:59 pm on Sunday, 7/29/12 • 	<ul style="list-style-type: none"> ○ Project Management Code of Ethics ○ Project Management Interpersonal Skills 	<ul style="list-style-type: none"> • Read PMBOK – Appendix G • Review PMP Exam Prep – Chapters, 13 and 14 • Individual Assignment 11 • Individual Assessment 11
13 8/8/12	<ul style="list-style-type: none"> • Final Exam • Due no later than 11:59 pm on Friday, 8/8/12 	Final Exam	

STATEMENT REGARDING PROFESSIONAL CONDUCT

Ferris students are expected to conduct themselves in a manner that is conducive to continued growth toward a business and/or professional career. Each student is expected to access classes regularly and to be fully prepared. All students are expected to act professionally and with a high

degree of ethical conduct while applying themselves fully to the job of learning. All communications are expected to be conducted in a professional manner, whether written or oral.

It is the student's obligation to know and observe all University policies and procedures and to keep current by reading the materials posted on the Ferris University Web Site and in its printed policies and bulletins.

STATEMENT REGARDING ACADEMIC MISCONDUCT

Plagiarism, unauthorized collusion on examinations, theft, sale, purchase or other unauthorized procurement of examinations or essay material, use of unauthorized aids while taking an examination, having someone else take an exam in your place or submitting for credit any paper not written by student, taking an exam for another student, copying of "do not copy" designated library materials, copying copyrighted software and destruction of equipment by introducing a computer virus and other similar actions are considered to be academic misconduct and unacceptable for students enrolled at Ferris State University.

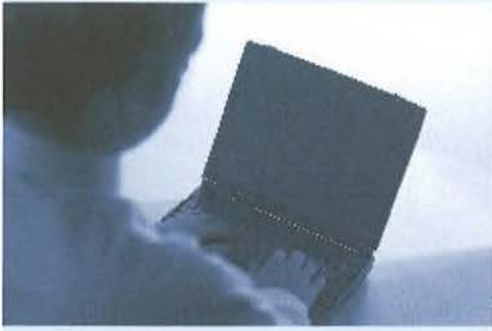
STATEMENT REGARDING DIVERSITY

This course embraces the Ferris Core Values of diversity by providing an environment which is supportive, safe and welcoming. We will listen respectfully to a diversity of ideas, beliefs and cultures presented by the members of the class.

Core Values

- **Collaboration:** Ferris contributes to the advancement of society by building partnerships with students, alumni, business and industry, government bodies, accrediting agencies, and the communities the University serves.
- **Diversity:** By providing a campus which is supportive, safe, and welcoming, Ferris embraces a diversity of ideas, beliefs, and cultures.
- **Ethical Community:** Ferris recognizes the inherent dignity of each member of the University community and treats everyone with respect. Our actions are guided by fairness, honesty, and integrity.
- **Excellence:** Committed to innovation and creativity, Ferris strives to produce the highest quality outcomes in all its endeavors.
- **Learning:** Ferris State University values education that is career-oriented, balances theory and practice, develops critical thinking, emphasizes active learning, and fosters responsibility and the desire for the lifelong pursuit of knowledge.
- **Opportunity:** Ferris, with a focus on developing career skills and knowledge, provides opportunities for civic engagement, leadership development, advancement, and success.

COB Syllabus Attachment is posted separately.



Ferris State University

College of Business

COURSE: ISIN 302 Business Intelligence in Health Care

INSTRUCTOR: Barbara L Ciaramitaro, PhD, PMP, CISSP, CSSLP

ONLINE INSTRUCTION : FerrisConnect
COURSE DATES: May 15 to August 8, 2012

OFFICE HOURS: Available by appointment.

Syllabus Changes: I reserve the right to make adjustment in this syllabus whenever I judge that the adjusted syllabus will better serve the overall learning needs of the class.

Please note that Ferris Connect Mail will be used for all course communications.

PHONE (OFFICE): (231) 591-3199 or (313) 207-6127 (preferred)

EMAIL ADDRESS: ciaramb@ferris.edu or Barbara.L.Ciaramitaro@verizon.net

FACEBOOK: Barbara L. Ciaramitaro

TWITTER: <http://twitter.com/bciaramitaro>

LINKEDIN:

<http://www.linkedin.com/in/barbaraciaramitaro>

BLOGS: <http://techademia.wordpress.com/> and <http://allthingsdigital.wordpress.com>

COURSE DESCRIPTION:

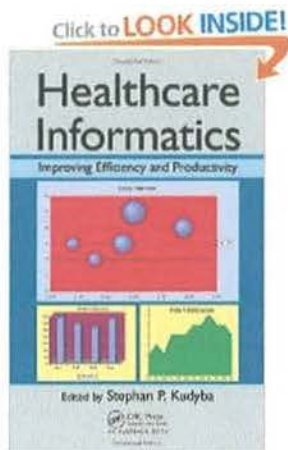
The course will provide best practices on the use of Business Intelligence methodology, processes and technologies in the healthcare domain. We will examine the history of business intelligence and its technology and process components. We will discuss Business Intelligence analysis tools such as data mining and performance management in the healthcare environment. This course will focus on how business intelligence can assist health care organizations in achieving improved quality of care and demonstrate evidence based medicine.

PREREQUISITES:

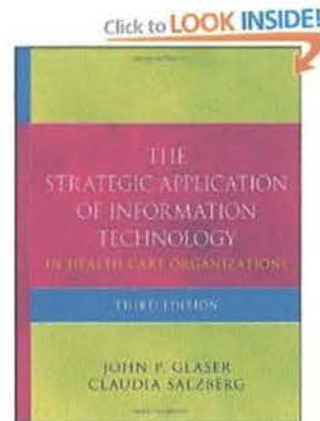
- None

COURSE MATERIALS:

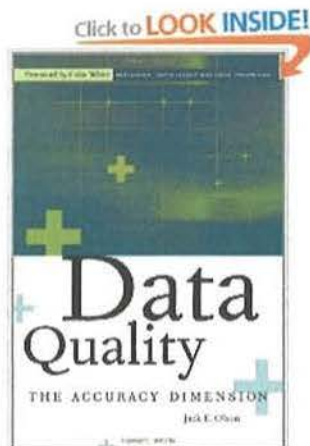
► **TEXTBOOK(S): REQUIRED**



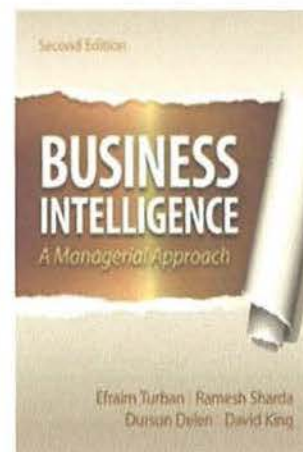
Title: Healthcare Informatics: Improving Efficiency and Productivity
Author: Stephan Kudyba
Publisher: CRC Press
ISBN 978-1439809785



Title: The Strategic Application of Information Technology in Health Care Organizations
Author: John Glaser and Claudia Salzberg
Publisher: Jossey Bass
ISBN: 978-0470639412



Title: Data Quality: The Accuracy Dimension
Author: Jack Olson
Publisher: Morgan Kaufman
ISBN: 978-1558608917



Title: Business Intelligence: A Managerial Approach
Second Edition
Author: Efraim Turban, et al
Publisher: Prentice Hall
ISBN: 978-0136100669

▶OTHER COURSE MATERIALS:

COURSE METHODS & OBJECTIVES:

▶COURSE METHODS:

▶COURSE OBJECTIVES:

- Online Lectures and Presentations
- Discussion Forum
- Individual Assignments
- Group Projects
- Midterm and Final Exams

- Understand the history and purpose of Business Intelligence
- Examine the Business Intelligence components: architecture, databases, data warehouses, performance management, and reporting & querying.
- Assess the use of data mining and analytics in Health Care environments
- Evaluate the use of Business Intelligence in each of the 7 stages of EMR (Electronic Medical Records) adoption.
- Assess how Business Intelligence processes and technologies can assist in achieving higher levels of “quality of care” in health care organizations
- Assess how Business Intelligence processes and technologies can assist in achieving demonstrating “evidence based medicine” in health care organizations
- Explore the major issues in implementing Business Intelligence in health care organizations
- Explore the use of Business Intelligence technology tools in health care.

ASSESSMENT GUIDELINES:

► ASSIGNMENTS:

The purpose of assignments is to reinforce the learning process. **All assignments are due Sunday of each week by 11:59 PM unless otherwise stated.**

► QUIZZES & EXAMS:

There will be a mid-term and final exam. The exams are cumulative. They are a combination of multiple choice and short essay questions.

For this online class, exams will be open-book and open-notes.

►DISCUSSIONS:

Students will be required to participate and interact with one another during the semester on the course discussion boards. Discussion questions will be posted on a weekly basis. You are required to create at least one original reply to the discussion topic and respond to at least two of your classmates for each discussion question posted. Early posting in the Discussion will ensure you receive replies from fellow students. Your weekly discussion posting will be graded using the following grading rubric.

Discussion Questions Grading Rubric

Points	Description
15 points	Responded to all questions with interaction among other students. Responses began early and were often. Responses were thoughtful and topical. Outside sources, previous knowledge, and real life experience were used in responses. The flow and direction of the discussion was greatly affected by contribution.
10-14 points	Did not respond directly to all questions, and/or did not respond to others with comments or questions and/or all responses are made in one visit to the site. Responses lacked deep analysis or thought..
9 or less points	Minimal participation. Did not respond to all posted questions. All responses are made in one visit to the site. Responses lacked analysis or thoughtfulness (applied text or lecture teaching points or real life examples) and/or was not topical (related to the text and lectures.)
0	No participation. No response

►MAKE-UP POLICY:

There will be no make up quizzes, exams, assignments or discussion question postings. It may be possible to pre-schedule a quiz or exam but students must contact the instructor directly and this will be determined on an individual basis.

COURSE POINTS & GRADING SCALE:

►COURSE POINTS:

Your performance in this course will be assessed as follows:

►GRADING SCALE:

950 and above = A
890 - 949 = A-
850 - 889 = B+
820 - 849 = B

			Assignment 2 <ul style="list-style-type: none"> Individual Assessment 2
3 5/28/12	<ul style="list-style-type: none"> Week #2 Discussion Board Individual Assignment 2 Individual Assessment 2 Due no later than 11:59 pm on Sunday, 5/27/12 	<ul style="list-style-type: none"> Business Intelligence Uses and Applications Business Analytics Data Visualization Data Mining 	<ul style="list-style-type: none"> Read Business Intelligence – Chapter 4 Read Data Quality – Chapters 6 to 7 Week #3 Discussion Board Individual Assignment 3 Individual Assessment 3
4 6/4/12	<ul style="list-style-type: none"> Week #3 Discussion Board Individual Assignment 3 Individual Assessment 3 Due no later than 11:59 pm on Sunday, 6/3/12 	<ul style="list-style-type: none"> Business Performance Management 	<ul style="list-style-type: none"> Read Business Intelligence – Chapter 5 Read Data Quality – Chapters 9 to 10 Week #4 Discussion Board Individual Assignment 4 Individual Assessment 4
5 6/11/12	<ul style="list-style-type: none"> Week #4 Discussion Board Individual Assignment 4 Individual Assessment 4 Due no later than 11:59 pm on Sunday, 	<ul style="list-style-type: none"> Implementing Business Intelligence 	<ul style="list-style-type: none"> Read Business Intelligence – Chapter 6 Read Data Quality – Chapters 9 to 10 Week #5 Discussion Board

Assessment	Points
Mid-Term and Final Exam (100 pts) =	200
Individual Assignments (11 @ 25 pts each)=	275
Individual Assessments (11@ 20 points each)	220
Discussion Board (11 @ 15 Points each) =	165
Final Paper	140
Total Pointes	1000

780 - 819 = B-
750 - 779 = C+
700 - 749 = C
650 - 699 = C-
600 - 649 = D+
550 - 599 = D
below 550 = F

CLASS SCHEDULE:

WEEK BEGINS	DUE	THIS WEEK'S TOPICS	ASSIGNED THIS WEEK
1 5/15/12		<ul style="list-style-type: none"> Introduction to Business Intelligence 	<ul style="list-style-type: none"> Read Business Intelligence – Chapters 1 and 2 Read Data Quality – Chapters 1 and 2 Week #1 Discussion Board Individual Assignment 1 Individual Assessment 1
2 5/21/12	<ul style="list-style-type: none"> Week #1 Discussion Board Individual Assignment 1 Individual Assessment 1 Due no later than 11:59 pm on Sunday, 5/20/12 	<ul style="list-style-type: none"> The Technology Side of Business Intelligence 	<ul style="list-style-type: none"> Read Business Intelligence – Chapters 3 and 4 Read Data Quality – Chapters 3 to 5 Week #2 Discussion Board Individual

	6/10/12		<ul style="list-style-type: none"> • Individual Assignment 5 • Individual Assessment 5
6 6/18/12	<ul style="list-style-type: none"> • Week #5 Discussion Board • Individual Assignment 5 • Individual Assessment 5 • Due no later than 11:59 pm on Sunday, 6/17/12 	<ul style="list-style-type: none"> • Managing Data Quality 	<ul style="list-style-type: none"> • Read Data Quality – Chapters 11 to 13 • Week #6 Discussion Board • Individual Assignment 6 • Individual Assessment 6
7 6/27/12	<ul style="list-style-type: none"> • Week #6 Discussion Board • Individual Assignment 6 • Individual Assessment 6 • Due no later than 11:59 pm on Sunday, 6/26/12 	<ul style="list-style-type: none"> • Implementing a Data Quality Plan 	<ul style="list-style-type: none"> • Mid Term
8 7/2/12	<ul style="list-style-type: none"> • Mid-Term • Due no later than 11:59 pm on Sunday, 7/1/12 	<ul style="list-style-type: none"> • Introduction to Business Intelligence in the Health Care Environment • Introduction to Health Care Informatics 	<ul style="list-style-type: none"> • Read Health Care Informatics Chapters 1, 2 and 9 • Read The Strategic Application of Information Technology in Health Care Organizatio

			<p>ns – Chapters 1, 2 and 3</p> <ul style="list-style-type: none"> • Week #8 Discussion Board • Individual Assignment 7 • Individual Assessment 7
<p>9 7/9/12</p>	<ul style="list-style-type: none"> • Week #8 Discussion Board • Individual Assignment 7 • Individual Assessment 7 • Due no later than 11:59 pm on Sunday, 7/8/12 	<ul style="list-style-type: none"> • Case Studies and Applications of Business Intelligence in Health Care <ul style="list-style-type: none"> ○ Health Care Analytics 	<ul style="list-style-type: none"> • Read Health Care Informatics Chapters 8 • Week #9 Discussion Board • Individual Assignment 8 • Individual Assessment 8
<p>10 7/15/12</p>	<ul style="list-style-type: none"> • Week #9 Discussion Board • Individual Assignment 8 • Individual Assessment 8 • Due no later than 11:59 pm on Sunday, 7/14/12 	<ul style="list-style-type: none"> • Case Studies and Applications of Business Intelligence in Health Care <ul style="list-style-type: none"> ○ Data Mining 	<ul style="list-style-type: none"> • Read Health Care Informatics Chapter 11 • Week #10 Discussion Board • Individual Assignment 9 • Individual Assessment 9
<p>11 7/22/12</p>	<ul style="list-style-type: none"> • Week #10 Discussion Board • Individual Assignment 9 • Individual Assessment 9 • Due no later than 11:59 pm on 	<ul style="list-style-type: none"> • Case Studies and Applications of Business Intelligence in Health Care <ul style="list-style-type: none"> ○ Improving Quality and Patient Care ○ Decision Support ○ Cost Savings 	<ul style="list-style-type: none"> • Read Health Care Informatics Chapter 10, 12 & 13 • Week #11 Discussion Board • Individual Assignment

	Sunday, 7/21/12		10 • Individual Assessment 10
12 7/30/12	<ul style="list-style-type: none"> • Week #11 Discussion Board • Individual Assignment 10 • Individual Assessment 10 • Due no later than 11:59 pm on Sunday, 7/29/12 • 	<ul style="list-style-type: none"> • Case Studies and Applications of Business Intelligence in Health Care <ul style="list-style-type: none"> ○ High Performance Medicine ○ Personalized Medicine ○ Health Care Reform 	<ul style="list-style-type: none"> • Read Health Care Informatics Chapters 6, 7 & 9 and 13 • Week #12 Discussion Board • Individual Assignment 11 • Individual Assessment 11
13 8/8/12	<ul style="list-style-type: none"> • Final Exam • Due no later than 11:59 pm on Friday, 8/8/12 	Final Exam	

STATEMENT REGARDING PROFESSIONAL CONDUCT

Ferris students are expected to conduct themselves in a manner that is conducive to continued growth toward a business and/or professional career. Each student is expected to access classes regularly and to be fully prepared. All students are expected to act professionally and with a high degree of ethical conduct while applying themselves fully to the job of learning. All communications are expected to be conducted in a professional manner, whether written or oral.

It is the student's obligation to know and observe all University policies and procedures and to keep current by reading the materials posted on the Ferris University Web Site and in its printed policies and bulletins.

STATEMENT REGARDING ACADEMIC MISCONDUCT

Plagiarism, unauthorized collusion on examinations, theft, sale, purchase or other unauthorized procurement of examinations or essay material, use of unauthorized aids while taking an examination, having someone else take an exam in your place or submitting for credit any paper not written by student, taking an exam for another student, copying of "do not copy" designated library materials, copying copyrighted software and destruction of equipment by introducing a computer virus and other similar actions are considered to be academic misconduct and unacceptable for students enrolled at Ferris State University.

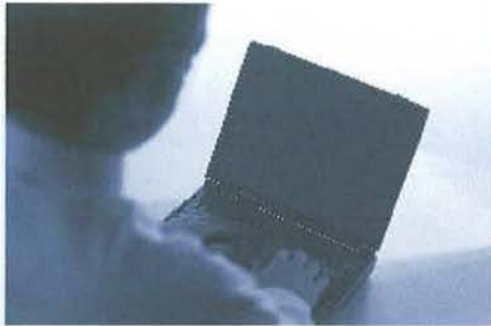
STATEMENT REGARDING DIVERSITY

This course embraces the Ferris Core Values of diversity by providing an environment which is supportive, safe and welcoming. We will listen respectfully to a diversity of ideas, beliefs and cultures presented by the members of the class.

Core Values

- **Collaboration:** Ferris contributes to the advancement of society by building partnerships with students, alumni, business and industry, government bodies, accrediting agencies, and the communities the University serves.
- **Diversity:** By providing a campus which is supportive, safe, and welcoming, Ferris embraces a diversity of ideas, beliefs, and cultures.
- **Ethical Community:** Ferris recognizes the inherent dignity of each member of the University community and treats everyone with respect. Our actions are guided by fairness, honesty, and integrity.
- **Excellence:** Committed to innovation and creativity, Ferris strives to produce the highest quality outcomes in all its endeavors.
- **Learning:** Ferris State University values education that is career-oriented, balances theory and practice, develops critical thinking, emphasizes active learning, and fosters responsibility and the desire for the lifelong pursuit of knowledge.
- **Opportunity:** Ferris, with a focus on developing career skills and knowledge, provides opportunities for civic engagement, leadership development, advancement, and success.

COB Syllabus Attachment is posted separately.



Ferris State University
College of Business
**COURSE: ISIN 390 Special Topics:
Virtual Worlds and Social Media**

INSTRUCTOR: Barbara L Ciaramitaro,
PhD, PMP, CISSP, CSSLP

COURSE DATES: January 11 to March
2, 2010

ONLINE DELIVERY: FerrisConnect

OFFICE HOURS: 1:00 to 3:00 pm
Tuesday in Big Rapids. Online office
hours will be posted each week. Other
times available by appointment.

Syllabus Changes: I reserve the right to
make adjustment in this syllabus
whenever I judge that the adjusted
syllabus will better serve the overall
learning needs of the class.

**Please note that Ferris Connect Mail
will be used for all course
communications.**

Emergency Preparedness: In the event
that students or the instructor are advised
not to attend class due to a health or
other emergency, please be aware that
all course material and assignments will
be posted on FerrisConnect. Depending
on the severity of the situation, alternative
virtual meetings or conferences may be
scheduled.

PHONE (OFFICE): (231) 591-3199

EMAIL ADDRESS: ciaramb@ferris.edu

FACEBOOK: Barbara L. Ciaramitaro

TWITTER: <http://twitter.com/bciaramitaro>

LINKEDIN:

<http://www.linkedin.com/in/barbaraciaramitaro>

BLOGS: <http://techademia.wordpress.com/> and
<http://allthingsdigital.wordpress.com>

COURSE DESCRIPTION:

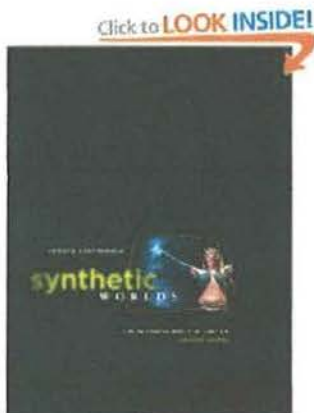
This course will be conducted in an online environment using Ferris Connect This course will present current research and knowledge on various aspects of the use of virtual worlds and social media by various domains including a discussion of the elements of virtual worlds, current examples of virtual worlds in use by various businesses and other organizations, the potential economic gains of utilizing virtual worlds, legal, security, privacy and technological issues, human factor issues in virtual worlds, and the future of virtual worlds and E-Commerce.

PREREQUISITES:

- ENGL150

COURSE MATERIALS:

►TEXTBOOK(S):



Title: Synthetic Worlds
Author: Edward Castronova
Publisher: University of Chicago Press
ISBN: 0226096270



Title: A Survival Guide to Social Media and Web 2.0 Optimization
Author: Deltina Hay
Publisher: Dalton Publishing
ISBN: 0981744389

COURSE METHODS & OBJECTIVES:

►COURSE METHODS:

- Online Lectures and Presentations
- Discussion Forum
- Hands-On Exploration
- Individual Assignments
- Final Exam

►COURSE OBJECTIVES:

Outcome: Understand and experience the elements of virtual worlds and social media.

Assessment: Independent assignments including hands-on exploration of virtual world and social media environments, and discussion questions.

Outcome: Acquire a working knowledge of virtual world and social media tools and technologies.

Assessment: Independent assignments including hands-on exploration of virtual world and social media environments, and discussion questions.

Outcome: Understand the economic, social and human factors implications of virtual worlds and social media.

Assessment: Independent assignments and discussion questions.

Outcome: Acquire a working knowledge of the use of virtual worlds and social media in establishing relationships with customers and other stakeholders.

Assessment: Independent assignments and discussion questions.

Outcome: Apply virtual world and social media tools and techniques to problems in the legal, privacy and information security domains.

Assessment: Independent assignments and discussion questions.

Outcome: Develop an understanding of ethical issues related to the use of virtual worlds and social media.

Assessment: Individual Assignments and discussion questions.

ASSESSMENT GUIDELINES:

► ASSIGNMENTS:

The purpose of assignments is to reinforce the learning process. **All assignments are due Sunday of each week by 11:59 PM unless otherwise stated.**

►QUIZZES & EXAMS:

There will be a mid-term and final exam. The exams are cumulative and will be a combination of multiple choice and short essay. For this online class, exams will be open-book and open-notes.

►DISCUSSIONS:

Students will be required to participate and interact with one another during the semester on the online course discussion boards. Discussion questions will be posted on a weekly basis. You are required to create at least one original reply to the discussion topic and respond to at least two of your classmates for each discussion question posted. Early posting in the Discussion will ensure you receive replies from fellow students. Your weekly discussion posting will be graded using the following grading rubric.

Discussion Questions Grading Rubric

Points	Description
25 points	Responded to all questions with interaction among other students. Responses began early and were often. Responses were thoughtful and topical. Outside sources, previous knowledge, and real life experience were used in responses. The flow and direction of the discussion was greatly affected by contribution.
15 to 25 points	Did not respond directly to all questions, and/or did not respond to others with comments or questions and/or all responses are made in one visit to the site. Responses lacked deep analysis or thought..
14 or less points	Minimal participation. Did not respond to all posted questions. All responses are made in one visit to the site. Responses lacked analysis or thoughtfulness (applied text or lecture teaching points or real life examples) and/or was not topical (related to the text and lectures.)
0	No participation. No response

►MAKE-UP POLICY:

There will be no make up quizzes, exams, assignments or discussion question postings. It may be possible to pre-schedule a quiz or exam but students must contact the instructor directly and this will be determined on an individual basis.

COURSE POINTS & GRADING SCALE:

► COURSE POINTS:

Your performance in this course will be assessed as follows:

Assessment	Points
Final Exam	225
Individual Assignments (7 @ 50 pts each)=	350
Discussion Board (7 @ 25 Points each) =	175
Individual Research Paper	250
Total	1000

► GRADING SCALE:

950 and above = A
 890 - 949 = A-
 850 - 889 = B+
 820 - 849 = B
 780 - 819 = B-
 750 - 779 = C+
 700 - 749 = C
 650 - 699 = C-
 600 - 649 = D+
 550 - 599 = D
 below 550 = F

7-WEEK ASSIGNMENT SCHEDULE:

WEEK BEGINS	DUE	THIS WEEK'S TOPICS	ASSIGNED THIS WEEK
1 1/11/10		<ul style="list-style-type: none"> Review of Course Objectives Review of Syllabus Introduction to Introduction to Virtual Worlds 	<ul style="list-style-type: none"> Pre-Course Survey Read Survival Guide to Social Media – Chapters 1 and 2 Read Synthetic Worlds – Chapters 1 and

			Social Media
<p>4 2/1/10</p>	<ul style="list-style-type: none"> • Week #3 Discussion Board • Assignment 3 - Legal and Privacy Issues in Virtual Worlds and Social Media • Due no later than 11:59 pm on Sunday 1/31/10 	<ul style="list-style-type: none"> • Information Security Issues related to Virtual Worlds 	<ul style="list-style-type: none"> • Read Survival Guide to Social Media – Chapters 7, 8 and 9 • Read Synthetic Worlds – Chapters 7, 8 and 9 • Week #4 Discussion Board • Assignment 4 – Information Security Issues in Virtual Worlds and Social Media Assessment
<p>5 2/8/10</p>	<ul style="list-style-type: none"> • Week #4 Discussion Board • Assignment 4 – Information Security Issues in Virtual Worlds and Social Media Assessment • Due no later than 11:59 pm on Sunday 2/7/10 	<ul style="list-style-type: none"> • Use of Virtual Worlds and Social Media by For-Profit Companies • Use of Virtual Worlds and Social Media by the Military and Government • Use of Virtual Worlds and Social Media by Education and Health Care 	<ul style="list-style-type: none"> • Read Survival Guide to Social Media – Chapters 10 and 11 • Read Synthetic Worlds – Chapters 10 and 11 • Week #5 Discussion Board • Assessment #5 – Virtual Worlds and Social Media by For-Profit Companies, or by the Military and Government or Education and Health Care
<p>6 2/15/10</p>	<ul style="list-style-type: none"> • Week #5 Discussion 	<ul style="list-style-type: none"> • Economic Assessment of 	<ul style="list-style-type: none"> • Read Survival Guide to Social

		<ul style="list-style-type: none"> • Introduction to Social Media 	<p>2</p> <ul style="list-style-type: none"> • Week #1 Discussion Board • Assignment 1 – Exploration of Virtual Worlds and Social Media Sites
<p>2 1/18/10</p>	<ul style="list-style-type: none"> • Pre-Course Assessment • Week #1 Discussion Board • Assignment 1 – Exploration of Virtual Worlds and Social Media Sites • Due no later than 11:59 pm on Sunday 1/17/10 	<ul style="list-style-type: none"> • Evolution of E-Commerce to V-Commerce • Web 2.0 Tools and Technologies • Relationship Building through Virtual Worlds and Social Media 	<ul style="list-style-type: none"> • Read Survival Guide to Social Media – Chapters 3 and 4 • Read Synthetic Worlds – Chapters 3 and 4 • Week #2 Discussion Board • Assignment 2 - Using Virtual Worlds and Social Media to Build Relationships
<p>3 1/25/10</p>	<ul style="list-style-type: none"> • Week #2 Discussion Board • Assignment 2 - Using Virtual Worlds and Social Media to Build Relationships • Due no later than 11:59 pm on Sunday 1/24/10 	<ul style="list-style-type: none"> • Legal and Privacy Issues related to Virtual Worlds and Social Media 	<ul style="list-style-type: none"> • Read Survival Guide to Social Media – Chapters 5 and 6 • Read Synthetic Worlds – Chapters 5 and 6 • Week #3 Discussion Board • Assignment 3 – Legal and Privacy Issues in Virtual Worlds and

	<p>Board</p> <ul style="list-style-type: none"> • Assignment 7 – Research Assignment on the use of Virtual Worlds and Social Media by For-Profit Companies, the Military and Government, or Education and Health Care • Due no later than 11:59 pm on Sunday 2/14/10 	<p>Virtual Worlds and Social Media</p> <ul style="list-style-type: none"> • Future of Virtual Worlds and Social Media 	<p>Media – Chapters 12 and 13</p> <ul style="list-style-type: none"> • Read Synthetic Worlds – Chapters 12 and 13 • Week #6 Discussion Board • Assessment #6 – Future of Virtual Worlds
<p>7 2/22/10</p>	<ul style="list-style-type: none"> • Week #6 Discussion Board • Assessment #6 – Future of Virtual Worlds • Due no later than 11:59 pm on Sunday 2/21/10 	<ul style="list-style-type: none"> • Student research assignments on legal, human factors, privacy, and security issues related to virtual worlds and social media. 	<ul style="list-style-type: none"> • Read Survival Guide to Social Media – Chapters 14 • Week # 7 Discussion Board • Assessment # 7 – Summary of Virtual World and Social Media Adventures • Final Exam
<p>8 3/1/10</p>	<ul style="list-style-type: none"> • Week #7 Discussion Board • Assessment #7 - Summary of Virtual World and Social Media Adventures • Final Exam 		

	<ul style="list-style-type: none"> • Due no later than 11:59 pm on Monday 3/2/10 		
--	--	--	--

STATEMENT REGARDING PROFESSIONAL CONDUCT

Ferris students are expected to conduct themselves in a manner that is conducive to continued growth toward a business and/or professional career. Each student is expected to access classes regularly and to be fully prepared. All students are expected to act professionally and with a high degree of ethical conduct while applying themselves fully to the job of learning. All communications are expected to be conducted in a professional manner, whether written or oral.

It is the student's obligation to know and observe all University policies and procedures and to keep current by reading the materials posted on the Ferris University Web Site and in its printed policies and bulletins.

STATEMENT REGARDING ACADEMIC MISCONDUCT

Plagiarism, unauthorized collusion on examinations, theft, sale, purchase or other unauthorized procurement of examinations or essay material, use of unauthorized aids while taking an examination, having someone else take an exam in your place or submitting for credit any paper not written by student, taking an exam for another student, copying of "do not copy" designated library materials, copying copyrighted software and destruction of equipment by introducing a computer virus and other similar actions are considered to be academic misconduct and unacceptable for students enrolled at Ferris State University.

STATEMENT REGARDING DIVERSITY

This course embraces the Ferris Core Values of diversity by providing an environment which is supportive, safe and welcoming. We will listen respectfully to a diversity of ideas, beliefs and cultures presented by the members of the class.

Core Values

- **Collaboration:** Ferris contributes to the advancement of society by building partnerships with students, alumni, business and industry, government bodies, accrediting agencies, and the communities the University serves.
- **Diversity:** By providing a campus which is supportive, safe, and welcoming, Ferris embraces a diversity of ideas, beliefs, and cultures.

- **Ethical Community:** Ferris recognizes the inherent dignity of each member of the University community and treats everyone with respect. Our actions are guided by fairness, honesty, and integrity.
- **Excellence:** Committed to innovation and creativity, Ferris strives to produce the highest quality outcomes in all its endeavors.
- **Learning:** Ferris State University values education that is career-oriented, balances theory and practice, develops critical thinking, emphasizes active learning, and fosters responsibility and the desire for the lifelong pursuit of knowledge.
- **Opportunity:** Ferris, with a focus on developing career skills and knowledge, provides opportunities for civic engagement, leadership development, advancement, and success.



Professional Development Certificate

Homeland Security Digital Security and Forensics

on the campus of Northwestern Michigan College

This certificate is a cooperative venture of the College of Business and the College of Education Criminal Justice Program. It was designed to increase the options available for students seeking to supplement their education in the field of homeland security.

This 12-credit hour certificate consists of four security courses. The courses are designed specifically to make the student a more thorough investigator in cyber crime scenes.

Admission Requirements

Any person who is admitted to the university is welcome to pursue this certificate.

Graduation Requirements

A Ferris student will receive this certificate after completion of the requirements for the certificate with a minimum 2.0 grade point average in the certificate courses.

No more than 50% of the credits required for this certificate may be transferred from another institution, nor will this certificate be granted if more than six of the certificate credits are specifically required in the student's major.

Course Requirements

Ferris State University	
HSCJ 202 Intro to Information Security	3
ISIN 300 Link and Visual Analysis.....	3

Choose One Track from Below:

<u>Law Enforcement Track</u>	
HSCJ 210 Intro to Digital Forensics	3
HSCJ 317 Fraud Examination.....	3

OR

<u>Technical Track</u>	
HSCJ 310 Digital Forensics and Analysis	3
HSCJ 315 Advanced Digital Forensics.....	3

Minimum credit hours required..... 12



For more information, call or visit us online.
866.857.1954 | FerrisNorth@ferris.edu | www.ferris.edu/statewide

Notice: Every effort has been made to include in this publication, information that, at the time of preparation for printing, is accurate. However, the contents of this publication are not to be regarded as a contract between students or potential students at Ferris State University. The University reserves the right to change at any time and without prior notice any provision or requirement including but not limited to, policies, tuition, fees, academic programs, or any other activity or matter. When describing programs offered by Ferris State University in this publication, the intent is to provide information on the type of career possibilities to which a curriculum may lead. In no way is this intended to imply a guarantee of job openings at a particular time for a particular student.

Project Management • Certificate

Why Choose Project Management?

Project management is a profession that consists of planning and executing projects within an organization. It is a field that is needed in many types of businesses including information technology, construction, health care, finance, marketing, manufacturing and others. The Project Management Certificate is a 12 credit hour certificate designed to prepare individuals for careers in project management in technical and non-technical fields. The certificate includes 4 courses that will provide an in-depth examination of project management practices, processes, tools and techniques. The first course in the certificate program examines the foundations of project management as defined by the Project Management Institute which is considered the premiere source for project management best practices and is the certifying body for both the PMP (Project Management Professional) and the CAPM (Certified Associate Project Management) designations. The first course consists of a review of the project management lifecycle and knowledge areas using resources such as the Project Management Body of Knowledge, course textbooks, and case studies. Following this foundation course, the next courses focus in more detail on specific aspects of project management including project scheduling, budgeting, risk management, communication, team management, and the procurement process. The final course places emphasis on preparation for project management certification exams including both the PMP (Project Management Professional) and the CAPM (Certified Associate in Project Management.)

This certificate is also offered through an online delivery format.

Get a Great Job

The Project Management certificate is designed to service one of the fastest growing and largest job classifications in both technical and non-technical fields. According to the Bureau of Labor Statistics (BLS), employment as a project manager is expected to continue to increase at a fast rate for the foreseeable future. Several surveys of job outlooks have also rated project management within the top 5 career paths currently and into the future. Certified project managers (PMP, CAPM) earn, on average, 15.6% more than their non-credentialed colleagues who have similar experience.

Admission Requirements

Applicants are expected to meet 3 of the 4 criteria listed below in order to be placed directly into a College of Business bachelor/associate degree program. Any mitigating circumstances will be considered on an individual basis by the College of Business Dean's Office.

- High school GPA of 2.5 (on a 4.0 scale)
- English ACT of 16 or higher or SAT of 370 or higher
- Math ACT of 19 or higher or SAT of 460 or higher
- Reading ACT of 19 or higher

Applicants not meeting the above criteria for direct admissions into a specific COB program, but still meeting Ferris State University admissions criteria, will be placed into the College of Business in the Pre-Business program until they meet the admission criteria for the program into which they desire entrance. Transfer student admission criteria can be found on the transfer student webpage.

Graduation Requirements

A Ferris student will receive the Project Management certificate upon graduation with a Baccalaureate degree, and after completion of the requirements for the certificate with a minimum of 2.0 grade point average in Project Management certificate courses.

No more than 50% of the credits in this certificate may be transferred from another institution, nor will the certificate be granted if more than 50% of the certificate credits are specifically required in the student's major.

Required Courses

		Credit Hours
PROJ 320	Proj Management Fundamentals	3
PROJ 350	Project Scheduling	3
PROJ 351	Project Communication	3
PROJ 420	Managing Procurement	3
	Minimum credit hours required	12



More Information

Accountancy, Finance & Information Systems
119 South Street, BUS 212
Big Rapids, MI 49307-2284
Phone: (231) 591-2434
Email: AFIS@ferris.edu

The College of Business is accredited by the Association of Collegiate Business Schools and Programs (ACBSP.)
http://www.acbsp.org/p/st/ld/sid=s1_001

FERRIS STATE UNIVERSITY

C O L L E G E O F B U S I N E S S

Appendix D: ISIN Checksheets



Bachelor of Science

INFORMATION SECURITY & INTELLIGENCE

Main (Big Rapids) Campus

As the only program of its kind in the country, Ferris Information Security & Intelligence (ISI) Program is at the forefront in its response to the need for skilled workers in Information Security/Data Analysis/Digital Investigation and Forensics. Developed with input from the U.S. Department of Homeland Security, the Pentagon, and investigative agencies; providing hands on utilization of state of the art technology, this program is uniquely positioned to satisfy the education credential necessary for students to be licensed as Professional Investigators in the State of Michigan, while our computer forensics coursework is accepted for meeting the education requirement to site for computer forensic examinations. In June 2011, Ferris State University formally received its designation as National Center of Academic Excellence in IA Education (CAE/IAE) by the NSA (National Security Agency) and the DHS (Department of Homeland Security). Ferris successfully mapped its ISI (Information Security & Intelligence) and ISM (Information System Management) programs classes against all six NSA standards making it one of very few universities in the country to have achieved that level of mapping and the CAE/IAE designation.

General Admission Criteria

To be admitted to this program you must have a high school cumulative GPA of 3.0 and an ACT score of 22, or a 2.7 cumulative GPA as a transfer student. You will need to submit official transcripts from all colleges/university with your application.

Course Requirements

General Education Requirements

COMM 105 Interpersonal Communication or	
COMM 121 Fundamentals Public Speaking	3
ENG 150 Composition	3
ENG 211 Business Writing	3
ENG 311 or 321 or 325 Advanced Writing	3
Scientific Understanding w/Lab	4
Scientific Understanding without Lab	3
Cultural Enrichment Electives	9
Social Awareness Electives	9
MATH 115 Intermediate Algebra	3

Business Core Courses

STQM 260 Statistics	3
ACT 201 Principles of Accounting I	4
MGMT 301 Applied Management	3
MKTG 3211 Principles of Marketing	3
MGMT 350 Tools for Decision Making	3

Ferris State University

Information Security & Intelligence Major Core

STQM 270 Introduction to Data Mining	3
STQM 360 Risk Analysis and Strategy	3
ISIN 200 All Things Digital	3
HSCJ 202 Principles of Information Security	3
HSCJ 310 Digital Forensics and Incident Response	3
PROJ 320 Project Management Fundamentals	3
HSCJ 317 Fraud Examination	3
ISIN 429 Legal and Ethical Issues in Security	3
ISIN 300 Visual Analysis	3
ISYS 200 Database Design	3
ISIN 301 Data Intelligence Competitive Theory	3
ISIN 312 Applications of Information Security	3
ISIN 390 Special Topics in Information Security	3
ISIN 491 Internship	3

ISIN 499 Capstone (Senior Standing)	3
Directed Electives	7

Available ISI Concentrations

Digital Forensics

HSCJ 315 Advanced Digital Forensics	3
ISYS 216 Java	3
ISYS 325 Networking Essentials	3
ISYS 371 Advanced Database	3

Network Security

ISYS 277 Linux Network Administration	3
ISYS 325 Networking Essentials	3
Approved Elective	3
Approved Elective	3

Project Management (Online)

PROJ 350 Project Scheduling	3
ISYS 351 Project Communication	3
PROJ 420 Project Procurement & PMP Prep	3
MGMT 370 Quality Operations Management	3

Foreign Language

Foreign Language Classes	12
--------------------------------	----

Total Gen Ed Credits	40
Total Business Core Credits	16
Total ISI Core Credits	45
Total Concentration Credits	12
Directed Electives Credits	7
TOTAL CREDITS	120

For more information, visit us online.

www.ferris.edu

Notice: Every effort has been made to include in this publication, information that, at the time of preparation for printing, is accurate. However, the contents of this publication are not to be regarded as a contract between students or potential students at Ferris State University. The University reserves the right to change at any time and without prior notice any provision or requirement including but not limited to, policies, tuition, fees, academic programs, or any other activity or matter. When describing programs offered by Ferris State University in this publication, the intent is to provide information on the type of career possibilities to which a curriculum may lead. In no way is this intended to imply a guarantee of job openings at a particular time for a particular student.

Ferris State University - College of Business
BACHELOR OF SCIENCE DEGREE IN INFORMATION SECURITY & INTELLIGENCE
120 Credits Required

NAME: _____ **ID#:** _____

REQUIRED	COURSE TITLE - PREREQUISITES SHOWN IN BRACKETS ()		S.H.	GRADE
General Education Requirements (40-41 hours)			40-41	
COMMUNICATION COMPETENCE - 12 Credits Required				
Consult the Ferris website: www.ferris.edu/htmls/academics/gened/bscomm.html.html for level approved courses				
COMM	105 or 121 or 201	Interpersonal Communication Fundamentals of Public Speaking Public Presentation Practice	3	
ENGL	150	English 1 (ENGL 074 w/C- or better or 14> ACT or 370 > SAT)	3	
ENGL	250	English 2 (ENGL 150 w/C- or better)	3	
ENGL	311 or 321 or 325	Advanced Technical Writing (ENGL 250 or ENGL 211 w/C or better) Advanced Composition (ENGL 250 or ENGL 211 w/C or better) Advanced Business Writing (ENGL 250 or ENGL 211 w/C or better)	3	
SCIENTIFIC UNDERSTANDING - 7 to 8 Credits Required				
Consult the Ferris website: www.ferris.edu/htmls/academics/gened/scicourses.html for approved courses.				
		Scientific Understanding w/ lab	4	
		Scientific Understanding Elective (lab or non-lab)	3 or 4	
QUANTITATIVE SKILLS - 3 Credits Required				
Consult the Ferris website: www.ferris.edu/htmls/academics/gened/bsquant.html for approved courses.				
MATH	115	Intermediate Algebra (Undergraduate level MATH 110 Minimum Grade of C- or ACT Math 19 or SAT Mathematics (old) 460 or Algebra 1--Supplemental Math 16 or Algebra 2-Supplemental Math 1 or SAT1 Math 460) If MATH ACT is 24 or higher, substitute a general education elective.	3	
CULTURAL ENRICHMENT - 9 Credits Required				
Consult the Ferris website: www.ferris.edu/htmls/academics/gened/cultcourses.html for approved courses				
		Cultural Enrichment Elective (Foreign Language Recommended)	3	
		Cultural Enrichment Elective	3	
		Cultural Enrichment Elective (200 level or above)	3	
SOCIAL AWARENESS - 9 Credits Required*				
Consult the Ferris website: www.ferris.edu/htmls/academics/gened/socccourses.html for level approved courses				
		Social Awareness Elective	3	
		Social Awareness Elective	3	
		Social Awareness Elective (200 level or above)	3	
NOTICE REGARDING WITHDRAWAL, RE-ADMISSION AND INTERRUPTION OF STUDIES				
Students who return to the university after an interrupted enrollment (not including summer semester) must normally meet the requirements of the curriculum which are in effect at the time of their return, not the requirements which were in effect when they were originally admitted.				

* Race/Ethnicity/Gender may be satisfied by some Social Awareness courses. Consult with your advisor.

Advising Notes:

Global consciousness requirement satisfied by _____.

Race/ethnicity/gender requirement satisfied by _____.

FSUS requirement satisfied by _____.

A 2.00 cumulative GPA is required in the major, concentration and overall.

40 credit hours must be at the 3xx - 4xx level.

30 credit hours must be Ferris classes.

Ferris State University - College of Business
BACHELOR OF SCIENCE DEGREE IN INFORMATION SECURITY & INTELLIGENCE

REQUIRED	COURSE TITLE - PREREQUISITES SHOWN IN BRACKETS ()		S.H.	GRADE
Major Core and Concentration Requirements (72 credit hours)			72	
BUSINESS COURSES - 15 Credits Required				
ACCT	201	Principles of Accounting (MATH 110 w/C- or better or ACT 19 or SAT 460)	3	
STQM	260	Introduction to Statistics (MATH 115 or 24 ACT)	3	
MGMT	301	Applied Management	3	
MKTG	321	Principles of Marketing (sophomore status or instructor permission)	3	
MGMT	350	Tools for Decision Making	3	
INFORMATION SECURITY AND INTELLIGENCE MAJOR COURSES - 45 Credits Required				
STQM	270	Introduction to Data Mining (STQM 260 w/C- or better)	3	
STQM	360	Risk Analysis and Strategy (STQM 260 w/C- or better)	3	
ISIN	200	All Things Digital	3	
HSCJ	202	Introduction to Information Security (None)	3	
ISIN	312	Applications of Information Security (HSCJ 202)	3	
HSCJ	310	Digital Forensics and Analysis (HSCJ 202)	3	
ISYS	200	Database Design and Implementation	3	
HSCJ	317	Fraud Examination	3	
ISIN	429	Legal & Ethical Issues in Information Security	3	
ISIN	300	Visual Analysis and Investigations	3	
ISIN	301	Data Intelligence Competitive Theory (ISIN 300, ISYS 200)	3	
PROJ	320	Project Management Fundamentals	3	
ISIN	390	Special Topics in ISIN	3	
ISIN	491	Internship	3	
ISIN	499	Capstone Experience (Senior Standing)	3	
CONCENTRATION** or approved minor - 12 Credits Required - ADVISOR APPROVAL REQUIRED				
		Concentration Class 1	3	
		Concentration Class 2	3	
		Concentration Class 3	3	
		Concentration Class 4	3	
DIRECTED ELECTIVES - 7 to 8 Credits Required - ADVISOR APPROVAL REQUIRED				
Directed Electives (7-8 credit hours)			7-8	
		Directed Elective	3	
		Directed Elective	3	
		Directed Elective	1 or 2	
TOTAL CREDIT HOURS REQUIRED			120	

**Concentrations may be selected from one of the following options or a custom concentration may be developed with advisor approval.
 (all classes and concentrations may not be available at all campuses - Main Campus only options are indicated by ***)

Concentrations	Classes
Data Mining***	STQM 342, STQM 380, STQM 322, ISYS 371
GIS	GISC 225, GISC 282, GISC 382, ISYS 371
Digital Forensics	HSCJ 315, ISYS 216, ISYS 325, ISYS 371
Network Security	ISYS 277, ISYS 325, Elective, Elective
Project Management	PROJ 350, PROJ 351, PROJ 420, MGMT 370
Software Development	ISYS 216, ISYS 316, ISYS 204, ISYS 304
Applied Networking	ECNS 115, ECNS 125, ECNS 215, ECNS 225
Business	ACCT 202, FINC 322, MGMT 370, BLAW 321
Foreign Language	Transfer (12 credit hours)

Effective Fall 2011

Ferris State University
B.S. Degree in Information Security & Intelligence

*** Effective Fall 2011 ***

Big Rapids Campus

Student Checksheet

NAME: _____ ID#: _____ DATE _____ ADVISOR: _____

Major Core Requirements (60 credits):

Required Courses	Course Title– FSU Prerequisites Shown in Parentheses ()	FSU S. H.	Planned	Completed	Grade
ACCT 201	Principles of Accounting (MATH 110 w/C- or better or 19 on ACT or 460 on SAT or one of the following MATH courses 115 to 120, 126, 130, 132, 135)	3			
MGMT 301	Applied Management	3			
MKTG 321	Principles of Marketing (sophomore status or instructor permit)	3			
MGMT 350	Tools for Decision Making	3			
STQM 260	Introduction to Statistics (MATH 115, 116 or 117 or 24 ACT or 560 SAT)	3			
STQM 270	Introduction to Data Mining (STQM 260)	3			
STQM 360	Risk Analysis and Strategy (STQM 260)	3			
ISYS 200	Database Design & Implementation (ISYS 105 or demonstrated competency)	3			
PROJ 320	Project Management	3			
HSCJ 202	Principles of Information Security				
HSCJ 310	Digital Forensics and Analysis (HSCJ 202)	3			
HSCJ 317	Fraud Examination	3			
ISIN 200	All Things Digital	3			
ISIN 300	Visual Analysis and Investigations	3			
ISIN 301	Data Intelligence Competitive Theory (ISIN 300, ISYS 200)	3			
ISIN312	Applications of Information Security (HSCJ 202)	3			
ISIN 390	Special Topics in ISIN	3			
ISIN 429	Legal & Ethical Issues in Information Security	3			
ISIN 491	Internship	3			
ISIN 499	Capstone Experience (Senior Standing)	3			
	Total				
	Major Core Credits Required: 60 credits				
	Directed Electives: 7-8 Credits Required (to total 120 credits for the BS Degree)				
	Note: Discuss with Advisor - 300-400 level classes may be needed here to fulfill the 40 credit 300-400 level requirements in the degree				
		3			
		3			
		1-2			

Concentration or an approved minor (12 Credits Required)						
Digital Forensics						
HSCJ 315	Advanced Digital Forensics (HSCJ 310)		3			
ISYS 216	Intro to Java Programming (ISYS 110)		3			
ISYS 371	Advanced Database Design & Implementation (ISYS 200 & ISYS 216)		3			
ISYS 325	Networking Essentials (ISYS 105 or demonstrated competency)		3			
Network Security						
ISYS 277	Linux Network Administration		3			
ISYS 325	Networking Essentials (ISYS 105 or demonstrated competency)		3			
	Elective		3			
	Elective		3			
Project Management (Online)						
PROJ 350	Project Schedule, Cost and Risk Management		3			
PROJ 351	Project Communication, Team Building and Conflict Management		3			
PROJ 420	Managing the Procurement Process and Preparing for the PMP		3			
MGMT 370	Quality-Operations Management		3			
Foreign Language						
	Foreign Language 1		3			
	Foreign Language 2		3			
	Foreign Language 3		3			
	Foreign Language 4		3			

Updated: August 31, 2011
Effective: Fall 2011 Semester

General Education Requirements (40-41 Credits):

EARNED MACRAO STAMP: YES NO

Required Courses	Course Title FSU Prerequisites Shown in Parentheses ()	FSU S.H.	Planned	Completed	Grade
COMM ELEC	COMM 105, Interpersonal Communication or COMM 121, Fundamentals of Public Speaking	3			
ENGL 150	English 1 (ENGL 074 w/C- or better or 14 > ACT or 370 > SAT)	3			
ENGL 211 or ENGL 250	Industrial and Career Writing (ENGL 150 w/C- or better) English 2 (ENGL 150 w/C- or better)	3			
ENGL 311 or ENGL 321 or ENGL 325	Advanced Technical Writing (ENGL 250 or ENGL 211 w/C or better) Advanced Composition (ENGL 250 or ENGL 211 w/C or better) Advanced Business Writing (ENGL 250 or ENGL 211 w/C or better)	3			
Scientific Understanding – 7 to 8 Credits Required					
This requirement can be met with science courses in the following areas: Astronomy, Biology, Chemistry, Geology, Physical Science, Physics, or FSU's GEOG 111 or GEOG 121					
	Scientific Understanding Elective with Lab	4			
	Scientific Understanding Elective (Lab or Non-Lab)	3 or 4			
Quantitative Skills – This requirement can be completed by one of the following options: (1) pass Math 115 or higher, (2) pass course proficiency exam in Math 115 or higher, (3) pass the College Algebra CLEP exam, or (4) an ACT math subtest score of 24 or higher.					
MATH 115	Intermediate Algebra (ACT of 19-21 or SAT of 350- 450)	3			
Cultural Enrichment – 9 Credits Required					
Credits can be earned in one or more subject areas; however, one three-credit course must be at the 200 level or higher. Select from the following subject areas: Art, Art History, any foreign language (German, Spanish or French at NMC), History, Humanities, Literature, Music, Philosophy (but not Logic), or Theatre.					
	Cultural Enrichment Elective	3			
	Cultural Enrichment Elective	3			
	Cultural Enrichment Elective (200 level or above)	3			
Social Awareness – 9 Credits Required					
Subject areas include: Anthropology, Economics, Geography (but not Physical Geography; this course is considered a science elective), Political Science, Psychology or Sociology. Criteria: (1) One three-credit course must be 200-level or higher. (2) Must have two subject areas.					
	Social Awareness Elective	3			
	Social Awareness Elective	3			
	Social Awareness Elective (200 level or above)	3			
40-41 General Education Hours Required					

Advising Notes:

Global consciousness requirement satisfied by: _____

Race/Ethnicity/Gender requirement satisfied by: _____

Admission Requirements:

1. High school students must have a 3.0 cumulative GPA (on a 4.00 scale) and an ACT composite score of 22. College students must have a 2.70 cumulative GPA to be admitted to this program.
2. Apply online at www.ferris.edu/offcampus and submit official high school or college transcripts and ACT scores to Ferris State University, Office of admissions and records, 1201 Campus Drive CSS201, Big Rapids, MI. 49307-2288
3. Admission to NMC College is also essential since many courses in the degree are completed through NMC as a dual enrolled student.
4. Financial aid is available when dually enrolled in classes at Ferris State University and NMC College. All financial aid will only originate with FSU to cover costs at both institutions. For more information regarding the financial aid process contact the main campus Financial Aid Office

Updated: August 31, 2011

Effective: Fall 2011 Semester

at 231-591-2110. For general financial aid questions you can also go to finaid@ferris.edu or for community college consortium questions go to cnsrtfinaid@ferris.edu.

Graduation Requirements:

1. A minimum of 120 semester credits must be completed for graduation – 40 of which must be 300 level or higher.
2. A 2.0 cumulative GPA is required in the major, concentration and overall for completion of the ISI degree.
3. At least 30 FSU semester credits must be completed to fulfill FSU residency requirements.
4. Students must meet the University General Education Requirements

Ferris ISI Core Course Descriptions (3 credit classes)

HSCJ 202-Principles of Information Security

Students explore the concepts of information security from both historical and emerging perspectives. Topics include the capabilities and threats of technology to information security, computer crime, homeland security, as well as legal, ethical and professional issues. The history, nature, and extent of computer crime and the roles and responsibilities of the legal system will also be investigated.

HSCJ 310-Digital Forensics and Analysis

Students learn the fundamentals of digital evidence collection and analysis. Emphasis is on both the collection of digital evidence and on common analysis tasks. Students will utilize various digital forensic tools and techniques for collection and analysis of digital evidence.

HSCJ 315-Advanced Digital Forensics

Students explore advanced digital forensic techniques and develop skills to deal with situations requiring a sophisticated response. Emerging and next generation computer technologies and threats, as well as proactive security measures and threat prevention will also be investigated. Students will utilize several digital forensic tools and techniques for collection, analysis, and incident processing.

HSCJ 317-Fraud Examination

Students will examine the fundamental reasons of why people commit fraud. Participants will investigate and explore how opportunity, pressures and rationalization are linked together to foster an atmosphere that can allow fraud to occur. Additionally, students will learn basic examination techniques for discovering fraud and more importantly, how to deter fraud from taking place.

ISIN 200-All Things Digital

Students investigate various digital devices including computers, cameras, surveillance equipment, and small devices and how to utilize them to advance security objectives. Students also work with various forms of media to understand the capabilities of each. Communication methods and networking are also explored.

ISIN 300-Visual Analysis Investigations

Introduction to transforming information into a visual format for analysis, interpretation and reporting. Students learn to deal with investigative issues involved to gather information, digital implications and strategies for effectively dealing with data from multiple sources. Analysis of digital data such as phone and financial records, surveillance information and visual media.

ISIN 301-Data-intelligence Comp Theory

Students examine the scientific process as it applies to hypothesis development. Investigation includes the analysis of various approaches to explaining events and developing competing hypothesis. The role of data and information in the development and support of intelligence in organization, national and international realms is also studied.

ISIN 312-Applications of Information Security

Students apply the tools and concepts of information security to mitigate and respond to risks. The theory and operation of information security tools and techniques are discussed, and students design and test their application in a variety of scenarios. Topics include software-, hardware-, host-, and network-based solutions.

ISIN 390-Special Topics in ISIN

This course covers various topics taught by diverse faculty.

ISIN 429-Legal-Ethical Issues Information Security

This course is intended to investigate the legal and ethical issues in Information Security. Ethical practices, privacy, copyright and licensing issues are research. Issues dealing with proprietary and personal information, as well as electronic technologies will be studied. An understanding of current and future impact on information systems and management strategies will be explored.

ISIN 499-Capstone Experience

This course provides students with an opportunity to demonstrate the skills and knowledge they have obtained in their program through project and/or portfolio methodologies and how they would be utilized in the workplace. Students will also investigate how information security is incorporated in their chosen path.

ISYS 371-Adv. Database Design and Implementation

Emphasis is placed on Entity-Relationships and Relational models, data definition languages, and manipulation languages. Structured Query Language (SQL) is used to develop database objects such as databases, logs, tables, indexes, views, constraints, defaults, roles, rules, stored procedures, and triggers. Database design is reviewed. Application development and modeling tools are discussed. Projects requiring the development of integrated databases are assigned.

PROJ 320-Project Management

An in-depth study of project management techniques currently employed for business and information systems projects. Topical areas will include project organization, planning and administration control and leadership. The need for accurate estimating, scheduling, communicating and reporting will be stressed through the use of several cases/projects. Senior Status

STQM 360-Risk Analysis and Strategy

Introduction to risk analysis and strategic approaches, principles, practices, tools, technology, and software. Risk analysis tools and approaches (e.g. planning, structured risk assessment, research and information discovery, probability and expectation, prioritization). Risk strategies, disposition, decision support, human resource development/management, and improvement/change strategies and tools. Application of risk analysis software. Applications and case studies to industry-specific events and projects (e.g. sport entertainment, security).

STQM 270-Introduction to Data Mining

Explore the relationship between data mining, data warehousing, and organizational needs. Explore basic data mining processes, methods and tools in varied areas of application such as business, manufacturing, healthcare, education, criminal justice, or government. Explore knowledge requirements across varied application areas as well as robust data mining processes and tools to serve varied needs. Case studies illustrate varied knowledge needs and data mining processes, methods, and tools. Introduces basic data mining software (e.g. WEKA, Excel based, or SPSS based).



Bachelor of Science

INFORMATION SECURITY & INTELLIGENCE

Delta Community College – Transfer Guide

As the only program of its kind in the country, Ferris Information Security & Intelligence (ISI) Program is at the forefront in its response to the need for skilled workers in Information Security/Data Analysis/Digital Investigation and Forensics. Developed with input from the U.S. Department of Homeland Security, the Pentagon, and investigative agencies; providing hands on utilization of state of the art technology, this program is uniquely positioned to satisfy the education credential necessary for students to be licensed as Professional Investigators in the State of Michigan, while our computer forensics coursework is accepted for meeting the education requirement to site for computer forensic examinations. In June 2011, Ferris State University formally received its designation as National Center of Academic Excellence in IA Education (CAE/IAE) by the NSA (National Security Agency) and the DHS (Department of Homeland Security). Ferris successfully mapped its ISI (Information Security & Intelligence) and ISM (Information System Management) programs classes against all six NSA standards making it one of very few universities in the country to have achieved that level of mapping and the CAE/IAE designation.

General Admission Criteria

To be admitted to this program you must have a high school cumulative GPA of 3.0 and an ACT score of 22, or a 2.7 cumulative GPA as a transfer student. You will need to submit official transcripts from all colleges/university with your application.

Course Requirements

Delta Community College

General Education Requirements (satisfied by MACRAO Stamp)

SPH 100 Interpersonal Communication (COMM 105) or	
SPH 101 Fundamentals Public Speaking (COMM 121)	3
ENG 110 or ENG 120 Composition 1 (ENG 150)	3
ENG 270 Business Writing (ENG 211)	3
Scientific Understanding w/Lab	4
Scientific Understanding without Lab	3
Cultural Enrichment Electives.....	9
Social Awareness Electives.....	9
MATH 113 Intermediate Algebra (MATH 115)	3
(Students must satisfy Global Consciousness & Race, Ethnicity, Gender requirements if they do not receive a MACRAO stamp)	

Business Core Courses

BUS 221 or MAT 131 Statistics (STQM 260).....	3
ACC 110 Principles of Accounting 1 (ACT 201).....	4
MGT 205 Applied Management (MGMT 301).....	3
MKT 201 Principles of Marketing (MKTG 321)	3

Ferris State University

General Education Courses

ENG 311 or 321 or 325 Advanced Writing.....	3
---	---

Business Core Courses

MGMT 350 Tools for Decision Making	3
--	---

Information Security & Intelligence Major Core

STQM 270 Introduction to Data Mining.....	3
STQM 360 Risk Analysis and Strategy.....	3
ISIN 200 All Things Digital.....	3
HSCJ 202 Principles of Information Security	3
HSCJ 310 Digital Forensics and Incident Response.....	3
PROJ 320 Project Management Fundamentals	3
HSCJ 317 Fraud Examination.....	3
ISIN 429 Legal and Ethical Issues in Security	3
ISIN 300 Visual Analysis.....	3
ISYS 200 Database Design	3
ISIN 301 Data Intelligence Competitive Theory.....	3

ISIN 312 Applications of Information Security	3
ISIN 390 Special Topics in Information Security.....	3
ISIN 491 Internship.....	3
ISIN 499 Capstone (Senior Standing).....	3
Directed Electives	7

Available ISI Concentrations

Ferris State University (Delta courses in parenthesis)

Digital Forensics

HSCJ 315 Advanced Digital Forensics	3
ISYS 216 Java (CIS 259 or CIS 207).....	3
ISYS 325 Networking Essentials (CIS 287).....	3
ISYS 371 Advanced Database	3

Network Security

ISYS 277 Linux Network Administration.....	3
ISYS 325 Networking Essentials (CIS 287).....	3
Approved Elective	3
Approved Elective	3

Project Management (Online)

PROJ 350 Project Scheduling	3
ISYS 351 Project Communication	3
PROJ 420 Project Procurement & PMP Prep.....	3
MGMT 370 Quality Operations Management	3

Foreign Language

Foreign Language Classes.....	12
-------------------------------	----

Total Gen Ed Credits	40
Total Business Core Credits	16
Total ISI Core Credits.....	45
Total Concentration Credits.....	12
Directed Electives Credits.....	7
TOTAL CREDITS	120

For more information, call or visit us online.

1.800.998.3425 or 1.616.451.4777

www.ferris.edu/Statewide

Notice: Every effort has been made to include in this publication, information that, at the time of preparation for printing, is accurate. However, the contents of this publication are not to be regarded as a contract between students or potential students at Ferris State University. The University reserves the right to change at any time and without prior notice any provision or requirement including but not limited to, policies, tuition, fees, academic programs, or any other activity or matter. When describing programs offered by Ferris State University in this publication, the intent is to provide information on the type of career possibilities to which a curriculum may lead. In no way is this intended to imply a guarantee of job openings at a particular time for a particular student.

Ferris State University
B.S. Degree in Information Security & Intelligence
***** Effective Fall 2011 *****
Delta College
AAS in CST – Information Security & Technology Program
Student Checksheet

NAME: _____ ID#: _____ DATE _____ ADVISOR: _____

Major Core Requirements (60 credits): Delta College equivalent courses are identified in third column. **FSU classes are in bold.**
 Highlighted courses are available online.

Required Courses	Course Title– FSU Prerequisites Shown in Parentheses ()	Delta Equivalent Courses	FSU S. H.	Completed	Grade
ACCT 201	Principles of Accounting (MATH 110 w/C- or better or 19 on ACT or 460 on SAT or one of the following MATH courses 115 to 120, 126, 130, 132, 135)	ACC 211 (MTH 097 w/ C or better)	3		
MGMT 301	Applied Management	MGT 245	3		
MKTG 321	Principles of Marketing (sophomore status or instructor permit)	MGT 243	3		
MGMT 350	Tools for Decision Making	FSU class	3		
STQM 260	Introduction to Statistics (MATH 115, 116 or 117 or 24 ACT or 560 SAT)	MTH 208 (MTH 092, 096, 097, 119)	3		
STQM 270	Introduction to Data Mining (STQM 260)	FSU class	3		
STQM 360	Risk Analysis and Strategy (STQM 260)	FSU class	3		
ISYS 200	Database Design & Implementation (ISYS 105 or demonstrated competency)	CST 263 (CST 161, 163 and 260)	3		
PROJ 320	Project Management	FSU class	3		
HSCJ 202	Principles of Information Security	FSU class			
HSCJ 310	Digital Forensics and Analysis (HSCJ 202)	FSU class	3		
HSCJ 317	Fraud Examination	FSU class	3		
ISIN 200	All Things Digital	FSU class	3		
ISIN 300	Visual Analysis and Investigations	FSU class	3		
ISIN 301	Data Intelligence Competitive Theory (ISIN 300, ISYS 200)	FSU class	3		
ISIN312	Applications of Information Security (HSCJ 202)	FSU class	3		
ISIN 390	Special Topics in ISIN	FSU class	3		
ISIN 429	Legal & Ethical Issues in Information Security	FSU class	3		
ISIN 491	Internship	FSU class	3		
ISIN 499	Capstone Experience (Senior Standing)	FSU class	3		
Total Major Core Credits Required: 60 credits					
Directed Electives: 7-8 Credits Required (to total 120 credits for the BS Degree)					
Note: Discuss with Advisor - 300-400 level classes may be needed here to fulfill the 40 credit 300-400 level requirements in the degree					
		FSU or Delta	3		
		FSU or Delta	3		
		FSU or Delta	1-2		

Concentration or an approved minor (12 Credits Required)					
Digital Forensics					
HSCJ 315	Advanced Digital Forensics (HSCJ 310)	FSU Class	3		
ISYS 216	Intro to Java Programming (ISYS 110)	CST 183 (CST 170, 177, 180)	3		
ISYS 371	Advanced Database Design & Implementation (ISYS 200 & ISYS 216)	CST 159 & 259	3		
ISYS 325	Networking Essentials (ISYS 105 or demonstrated competency)	CST 161 (CST 133)	3		
GIS					
GISC 225	Principles of GIS	Ferris class	3		
GISC 282	Geographic Information Systems 2	Ferris class	3		
GISC 382	GIS Data Analysis	Ferris class	3		
ISYS 371	Adv Database Design-Implement	CST 159 & 259	3		
Applied Networking					
ECNS 115	Networks 1	CST 161 (CST 133)	3		
ECNS 125	Networks 2	CST 164 (CST 161)	3		
ECNS 215	Networks 3	CST 260 (CST 161)	3		
ECNS 225	Networks 4	CST 264 (CST 164 and 260)	3		
Network Security					
ISYS 277	Linux Network Administration	CST 265 (CST 165)	3		
ISYS 325	Networking Essentials (ISYS 105 or demonstrated competency)	CST 161 (CST 133)	3		
	Elective	CST 260 (CST 161)	3		
	Elective	CST 269 (CST 161, 164 and 260)	3		
Project Management (Online)					
PROJ 350	Project Schedule, Cost and Risk Management	Ferris class	3		
PROJ 351	Project Communication, Team Building and Conflict Management	Ferris class	3		
PROJ 420	Managing the Procurement Process and Preparing for the PMP	Ferris class	3		
MGMT 370	Quality-Operations Management	Ferris class	3		
Software Development					
ISYS 216	Intro to Java Programming (ISYS 110)	CST 183 (CST 170, 177, 180)	3		
ISYS 316	Advanced Java Programming	CST 180 (MATH LEVEL 5 and CST 177)	3		
ISYS 204	Introduction to Visual Basic	CST 271 (CST 171)	3		
ISYS 304	Advanced Visual Basic Program	CST 280 (CST 180, CST 181, CIS 170, CPS 170, EGR 170 or CPS 171)	3		
Foreign Language					
	Foreign Language 1		3		
	Foreign Language 2		3		
	Foreign Language 3		3		
	Foreign Language 4		3		

Updated: August 31, 2011
Effective: Fall 2011 Semester

General Education Requirements (40-41 Credits):

EARNED MACRAO STAMP: YES NO

Required Courses	Course Title FSU Prerequisites Shown in Parentheses ()	Delta Equivalent Courses	FSU S.H.	Completed	Grade
Communication Competence—12 Credits Required					
COMM ELEC	COMM 105, Interpersonal Communication or COMM 121, Fundamentals of Public Speaking	COM 112 or COM 114	3		
ENGL 150	English 1 (ENGL 074 w/C- or better or 14 > ACT or 370 > SAT)	ENG 111	3		
ENGL 211 or ENGL 250	Industrial and Career Writing (ENGL 150 w/C- or better) English 2 (ENGL 150 w/C- or better)	ENG 113 or 213 or ENG 112	3		
ENGL 311 or ENGL 321 or ENGL 325	Advanced Technical Writing (ENGL 250 or ENGL 211 w/C or better) Advanced Composition (ENGL 250 or ENGL 211 w/C or better) Advanced Business Writing (ENGL 250 or ENGL 211 w/C or better)	FSU Class	3		
Scientific Understanding – 7 to 8 Credits Required					
This requirement can be met with science courses in the following areas: Astronomy, Biology, Chemistry, Geology, Physical Science, Physics, or FSU's GEOG 111 or GEOG 121					
	Scientific Understanding Elective with Lab	Delta Lab Science	4		
	Scientific Understanding Elective (Lab or Non-Lab)	Delta	3 or 4		
Quantitative Skills – This requirement can be completed by one of the following options: (1) pass Math 115 or higher, (2) pass course proficiency exam in Math 115 or higher, (3) pass the College Algebra CLEP exam, or (4) an ACT math subtest score of 24 or higher.					
MATH 115	Intermediate Algebra (ACT of 19-21 or SAT of 350- 450)	MTH 119 or higher (MTH 092, 096, 097)	3		
Cultural Enrichment – 9 Credits Required					
Credits can be earned in one or more subject areas; however, one three-credit course must be at the 200 level or higher. Select from the following subject areas: Art, Art History, any foreign language (German, Spanish or French at Delta), History, Humanities, Literature, Music, Philosophy (but not Logic), or Theatre.					
	Cultural Enrichment Elective	Delta Elective	3		
	Cultural Enrichment Elective	Delta Elective	3		
	Cultural Enrichment Elective (200 level or above)	Delta Elective	3		
Social Awareness – 9 Credits Required					
Subject areas include: Anthropology, Economics, Geography (but not Physical Geography; this course is considered a science elective), Political Science, Psychology or Sociology. Criteria: (1) One three-credit course must be 200-level or higher. (2) Must have two subject areas.					
	Social Awareness Elective	Delta Elective	3		
	Social Awareness Elective	Delta Elective	3		
	Social Awareness Elective (200 level or above)	Delta Elective	3		
40-41 General Education Hours Required					
The University requires that one or more general education courses meet the Global Consciousness and Race, Ethnicity and Gender (REG) criteria. Students can take one course that meets both the Global and REG requirement simultaneously. Delta courses meeting the various criteria and that are particularly suited for the ISI degree are listed below:					
Cultural Enrichment: PHL 213, Introduction to Ethics			Global Consciousness and Social Awareness: GEO 113, World Cultural Geography		
Social Awareness: ECN 221, Principles of Economics I ECN 222, Principles of Economics II GEO 255, Third World Development or SOC 265, 3rd World Development			Global Consciousness and Cultural Enrichment: Foreign language course from Delta IHU 234, World Religions or SSI 234, World Religions		
Global Consciousness GEO 223, Geography of Europe POL 222, Politics of Middle East			REG and Social Awareness: POL 212, State & Local Government POL 225, World Politics PSY 211, General Psychology SOC 211, Principles of Sociology (SA Foundation Course) SOC 212, Social Problems (SA Foundation Course)		
Global, REG and Social Awareness: POL 221, Comparative Government SOC 231, Cultural Anthropology (SA Foundation Course)					

Updated: August 31, 2011
Effective: Fall 2011 Semester

Advising Notes:

Global consciousness requirement satisfied by: _____
Race/Ethnicity/Gender requirement satisfied by: _____

Admission Requirements:

1. High school students must have a 3.0 cumulative GPA (on a 4.00 scale) and an ACT composite score of 22. College students must have a 2.70 cumulative GPA to be admitted to this program.
2. Apply online at www.ferris.edu/offcampus and submit official high school or college transcripts and ACT scores to Ferris State University, Office of admissions and records, 1201 Campus Drive CSS201, Big Rapids, MI. 49307-2288
3. Admission to Delta College is also essential since many courses in the degree are completed through Delta as a dual enrolled student.
4. Financial aid is available when dually enrolled in classes at Ferris State University and Delta College. All financial aid will only originate with FSU to cover costs at both institutions. For more information regarding the financial aid process contact the main campus Financial Aid Office at 231-591-2110. For general financial aid questions you can also go to finaid@ferris.edu or for community college consortium questions go to cnsrtfinaid@ferris.edu.

Graduation Requirements:

1. A minimum of 120 semester credits must be completed for graduation – 40 of which must be 300 level or higher.
2. A 2.0 cumulative GPA is required in the major, concentration and overall for completion of the ISI degree.
3. At least 30 FSU semester credits must be completed to fulfill FSU residency requirements.
4. Students must meet the University General Education Requirements (*Refer to Delta guidance regarding meeting the Ferris General Education requirements and /or Delta MACRAO requirements*).

For more information or answers to your questions, contact us at:

Phone: 616.451.4777 or 800.998.3425
Fax: 616.451.4740
E-mail: fsugr@ferris.edu

Ferris State University – Grand Rapids
151 Fountain Street NE
Grand Rapids, MI 49503

Ferris ISI Core Course Descriptions (3 credit classes)

HSCJ 202-Principles of Information Security

Students explore the concepts of information security from both historical and emerging perspectives. Topics include the capabilities and threats of technology to information security, computer crime, homeland security, as well as legal, ethical and professional issues. The history, nature, and extent of computer crime and the roles and responsibilities of the legal system will also be investigated.

HSCJ 310-Digital Forensics and Analysis

Students learn the fundamentals of digital evidence collection and analysis. Emphasis is on both the collection of digital evidence and on common analysis tasks. Students will utilize various digital forensic tools and techniques for collection and analysis of digital evidence.

HSCJ 315-Advanced Digital Forensics

Students explore advanced digital forensic techniques and develop skills to deal with situations requiring a sophisticated response. Emerging and next generation computer technologies and threats, as well as proactive security measures and threat prevention will also be investigated. Students will utilize several digital forensic tools and techniques for collection, analysis, and incident processing.

HSCJ 317-Fraud Examination

Students will examine the fundamental reasons of why people commit fraud. Participants will investigate and explore how opportunity, pressures and rationalization are linked together to foster an atmosphere that can allow fraud to occur. Additionally, students will learn basic examination techniques for discovering fraud and more importantly, how to deter fraud from taking place.

ISIN 200-All Things Digital

Students investigate various digital devices including computers, cameras, surveillance equipment, and small devices and how to utilize them to advance security objectives. Students also work with various forms of media to understand the capabilities of each. Communication methods and networking are also explored.

ISIN 300-Visual Analysis Investigations

Introduction to transforming information into a visual format for analysis, interpretation and reporting. Students learn to deal with investigative issues involved to gather information, digital implications and strategies for effectively dealing with data from multiple sources. Analysis of digital data such as phone and financial records, surveillance information and visual media.

ISIN 301-Data-intelligence Comp Theory

Students examine the scientific process as it applies to hypothesis development. Investigation includes the analysis of various approaches to explaining events and developing competing hypothesis. The role of data and information in the development and support of intelligence in organization, national and international realms is also studied.

ISIN 312-Applications of Information Security

Students apply the tools and concepts of information security to mitigate and respond to risks. The theory and operation of information security tools and techniques are discussed, and students design and test their application in a variety of scenarios. Topics include software-, hardware-, host-, and network-based solutions.

ISIN 390-Special Topics in ISIN

This course covers various topics taught by diverse faculty.

ISIN 429-Legal-Ethical Issues Information Security

This course is intended to investigate the legal and ethical issues in Information Security. Ethical practices, privacy, copyright and licensing issues are research. Issues dealing with proprietary and personal information, as well as electronic technologies will be studied. An understanding of current and future impact on information systems and management strategies will be explored.

ISIN 499-Capstone Experience

This course provides students with an opportunity to demonstrate the skills and knowledge they have obtained in their program through project and/or portfolio methodologies and how they would be utilized in the workplace. Students will also investigate how information security is incorporated in their chosen path.

ISYS 371-Adv. Database Design and Implementation

Emphasis is placed on Entity-Relationships and Relational models, data definition languages, and manipulation languages. Structured Query Language (SQL) is used to develop database objects such as databases, logs, tables, indexes, views, constraints, defaults, roles, rules, stored procedures, and triggers. Database design is reviewed. Application development and modeling tools are discussed. Projects requiring the development of integrated databases are assigned.

PROJ 320-Project Management

An in-depth study of project management techniques currently employed for business and information systems projects. Topical areas will include project organization, planning and administration control and leadership. The need for accurate estimating, scheduling, communicating and reporting will be stressed through the use of several cases/projects. Senior Status

STQM 360-Risk Analysis and Strategy

Introduction to risk analysis and strategic approaches, principles, practices, tools, technology, and software. Risk analysis tools and approaches (e.g. planning, structured risk assessment, research and information discovery, probability and expectation, prioritization). Risk strategies, disposition, decision support, human resource development/management, and improvement/change strategies and tools. Application of risk analysis software. Applications and case studies to industry-specific events and projects (e.g. sport entertainment, security).

STQM 270-Introduction to Data Mining

Explore the relationship between data mining, data warehousing, and organizational needs. Explore basic data mining processes, methods and tools in varied areas of application such as business, manufacturing, healthcare, education, criminal justice, or government. Explore knowledge requirements across varied application areas as well as robust data mining processes and tools to serve varied needs. Case studies illustrate varied knowledge needs and data mining processes, methods, and tools. Introduces basic data mining software (e.g. WEKA, Excel based, or SPSS based).



Bachelor of Science

INFORMATION SECURITY & INTELLIGENCE

Grand Rapids Community College – Transfer Guide

As the only program of its kind in the country, Ferris Information Security & Intelligence (ISI) Program is at the forefront in its response to the need for skilled workers in Information Security/Data Analysis/Digital Investigation and Forensics. Developed with input from the U.S. Department of Homeland Security, the Pentagon, and investigative agencies; providing hands on utilization of state of the art technology, this program is uniquely positioned to satisfy the education credential necessary for students to be licensed as Professional Investigators in the State of Michigan, while our computer forensics coursework is accepted for meeting the education requirement to site for computer forensic examinations. In June 2011, Ferris State University formally received its designation as National Center of Academic Excellence in IA Education (CAE/IAE) by the NSA (National Security Agency) and the DHS (Department of Homeland Security). Ferris successfully mapped its ISI (Information Security & Intelligence) and ISM (Information System Management) programs classes against all six NSA standards making it one of very few universities in the country to have achieved that level of mapping and the CAE/IAE designation.

General Admission Criteria

To be admitted to this program you must have a high school cumulative GPA of 3.0 and an ACT score of 22, or a 2.7 cumulative GPA as a transfer student. You will need to submit official transcripts from all colleges/university with your application.

Course Requirements

Grand Rapids Community College

General Education Requirements (satisfied by MACRAO Stamp) (Ferris courses in parenthesis)

COM 135 Interpersonal Communication (COMM 105) or COM 131 Fundamentals Public Speaking (COMM 121)...	3
EN 100 or EN 101 Composition 1 (ENG 150).....	3
EN 102 English 2 (ENG 250).....	3
Scientific Understanding w/Lab.....	4
Scientific Understanding without Lab.....	3
Cultural Enrichment Electives.....	9
Social Awareness Electives.....	9
MA 107 Intermediate Algebra (MATH 115).....	3
(Students must satisfy Global Consciousness & Race, Ethnicity, Gender requirements if they do not receive a MACRAO stamp)	

Business Core Courses

BA 256 Principles of Accounting (ACCT 201).....	3
BA 254 or MAT 215 or PY 281 Statistics (STQM 260)...	3
BA 283 Applied Management (MGMT 301).....	3
BA 270 Principles of Marketing (MKTG 321).....	3

Ferris State University (GRCC courses in parenthesis)

General Education Courses

ENG 311 or 321 or 325 Advanced Writing.....	3
---	---

Business Core Courses

MGMT 350 Tools for Decision Making.....	3
---	---

Information Security & Intelligence Major Core

STQM 270 Introduction to Data Mining.....	3
STQM 360 Risk Analysis and Strategy.....	3
ISIN 200 All Things Digital.....	3
HSCJ 202 Principles of Information Security.....	3
HSCJ 310 Digital Forensics and Incident Response.....	3
PROJ 320 Project Management Fundamentals.....	3
HSCJ 317 Fraud Examination.....	3
ISIN 429 Legal and Ethical Issues in Security.....	3
ISIN 300 Visual Analysis.....	3
ISYS 200 Database Design (CO 171).....	3
ISIN 301 Data Intelligence Competitive Theory.....	3
ISIN 312 Applications of Information Security.....	3
ISIN 390 Special Topics in Information Security.....	3

ISIN 491 Internship.....	3
ISIN 499 Capstone (Senior Standing).....	3
Directed Electives.....	7

Available ISI Concentrations

Ferris State University (GRCC courses in parenthesis)

Digital Forensics

HSCJ 315 Advanced Digital Forensics.....	3
ISYS 216 Java (CO 117).....	3
ISYS 325 Networking Essentials (CO 231).....	3
ISYS 371 Advanced Database.....	3

Network Security

ISYS 277 Linux Network Administration (CO 232).....	3
ISYS 325 Networking Essentials (CO 231).....	3
Approved Elective.....	3
Approved Elective.....	3

Project Management (Online)

PROJ 350 Project Scheduling.....	3
ISYS 351 Project Communication.....	3
PROJ 420 Project Procurement & PMP Prep.....	3
MGMT 370 Quality Operations Management.....	3

National Security (Online)

ISIN 350 Organizational Planning and Security Measures...	3
ISIN 351 Global Security and Policy.....	3
ISIN 352 The Role of Intelligence.....	3
Approved Elective.....	3

Foreign Language

Foreign Language Classes.....	12
-------------------------------	----

Total Gen Ed Credits.....	40
Total Business Core Credits.....	16
Total ISI Core Credits.....	45
Total Concentration Credits.....	12
Directed Electives Credits.....	7
TOTAL CREDITS.....	120

For more information, call or visit us online.

1.800.998.3425 or 1.616.451.4777

www.ferris.edu/Statewide

Ferris State University
B.S. Degree in Information Security & Intelligence

*** Effective Fall 2011 ***

Grand Rapids Community College

Student Checksheet

NAME: _____ ID#: _____ DATE _____ ADVISOR: _____

Major Core Requirements (60 credits): GRCC College equivalent courses are identified in third column. FSU classes are in bold. Highlighted courses are available online.

Required Courses	Course Title- FSU Prerequisites Shown in Parentheses ()	GRCC Equivalent Courses	FSU S. H.	Planned	Completed	Grade
ACCT 201	Principles of Accounting (MATH 110 w/C- or better or 19 on ACT or 460 on SAT or one of the following MATH courses 115 to 120, 126, 130, 132, 135)	BA 256	3			
MGMT 301	Applied Management	BA 283	3			
MKTG 321	Principles of Marketing (sophomore status or instructor permit)	MGT 243	3			
MGMT 350	Tools for Decision Making	FSU class	3			
STQM 260	Introduction to Statistics (MATH 115, 116 or 117 or 24 ACT or 560 SAT)	BA 254 or MAT 215 or PY 281 Statistics	3			
STQM 270	Introduction to Data Mining (STQM 260)	FSU class	3			
STQM 360	Risk Analysis and Strategy (STQM 260)	FSU class	3			
ISYS 200	Database Design & Implementation (ISYS 105 or demonstrated competency)	CO 171	3			
PROJ 320	Project Management	FSU class	3			
HSCJ 202	Principles of Information Security	FSU class				
HSCJ 310	Digital Forensics and Analysis (HSCJ 202)	FSU class	3			
HSCJ 317	Fraud Examination	FSU class	3			
ISIN 200	All Things Digital	FSU class	3			
ISIN 300	Visual Analysis and Investigations	FSU class	3			
ISIN 301	Data Intelligence Competitive Theory (ISIN 300, ISYS 200)	FSU class	3			
ISIN312	Applications of Information Security (HSCJ 202)	FSU class	3			
ISIN 390	Special Topics in ISIN	FSU class	3			
ISIN 429	Legal & Ethical Issues in Information Security	FSU class	3			
ISIN 491	Internship	FSU class	3			
ISIN 499	Capstone Experience (Senior Standing)	FSU class	3			
	Total					
	Major Core Credits Required: 60 credits					
	Directed Electives: 7-8 Credits Required (to total 120 credits for the BS Degree)					
	Note: Discuss with Advisor - 300-400 level classes may be needed here to fulfill the 40 credit 300-400 level requirements in the degree					
		FSU or GRCC	3			
		FSU or GRCC	3			
		FSU or GRCC	1-2			

Concentration or an approved minor (12 Credits Required						
Digital Forensics						
HSCJ 315	Advanced Digital Forensics (HSCJ 310)	FSU Class	3			
ISYS 216	Intro to Java Programming (ISYS 110)	CO 117	3			
ISYS 371	Advanced Database Design & Implementation (ISYS 200 & ISYS 216)		3			
ISYS 325	Networking Essentials (ISYS 105 or demonstrated competency)	CO 231	3			
GIS						
GISC 225	Principles of GIS	Ferris class	3			
GISC 282	Geographic Information Systems 2	Ferris class	3			
GISC 382	GIS Data Analysis	Ferris class	3			
ISYS 371	Adv Database Design-Implement		3			
Network Security						
ISYS 277	Linux Network Administration	CO 232	3			
ISYS 325	Networking Essentials (ISYS 105 or demonstrated competency)	CO 231	3			
	Elective	CST 260 (CST 161)	3			
	Elective	CST 269 (CST 161, 164 and 260)	3			
Project Management (Online)						
PROJ 350	Project Schedule, Cost and Risk Management	Ferris class	3			
PROJ 351	Project Communication, Team Building and Conflict Management	Ferris class	3			
PROJ 420	Managing the Procurement Process and Preparing for the PMP	Ferris class	3			
MGMT 370	Quality-Operations Management	Ferris class	3			
Foreign Language						
	Foreign Language 1		3			
	Foreign Language 2		3			
	Foreign Language 3		3			
	Foreign Language 4		3			

Updated: August 31, 2011
Effective: Fall 2011 Semester

General Education Requirements (40-41 Credits):

EARNED MACRAO STAMP: YES NO

Required Courses	Course Title FSU Prerequisites Shown in Parentheses ()	GRCC Equivalent Courses	FSU S.H.	Planned	Completed	Grade
Communication Competence—12 Credits Required						
COMM ELEC	COMM 105, Interpersonal Communication or COMM 121, Fundamentals of Public Speaking	COM 135 or COM 131	3			
ENGL 150	English 1 (ENGL 074 w/C- or better or 14 > ACT or 370 > SAT)	EN 100 or EN 101	3			
ENGL 211 or ENGL 250	Industrial and Career Writing (ENGL 150 w/C- or better) English 2 (ENGL 150 w/C- or better)	BA 102	3			
ENGL 311 or ENGL 321 or ENGL 325	Advanced Technical Writing (ENGL 250 or ENGL 211 w/C or better) Advanced Composition (ENGL 250 or ENGL 211 w/C or better) Advanced Business Writing (ENGL 250 or ENGL 211 w/C or better)	FSU Class	3			
Scientific Understanding – 7 to 8 Credits Required This requirement can be met with science courses in the following areas: Astronomy, Biology, Chemistry, Geology, Physical Science, Physics, or FSU's GEOG 111 or GEOG 121						
	Scientific Understanding Elective with Lab		4			
	Scientific Understanding Elective (Lab or Non-Lab)		3 or 4			
Quantitative Skills – This requirement can be completed by one of the following options: (1) pass Math 115 or higher, (2) pass course proficiency exam in Math 115 or higher, (3) pass the College Algebra CLEP exam, or (4) an ACT math subtest score of 24 or higher.						
MATH 115	Intermediate Algebra (ACT of 19-21 or SAT of 350- 450)	MA 107	3			
Cultural Enrichment – 9 Credits Required Credits can be earned in one or more subject areas; however, one three-credit course must be at the 200 level or higher. Select from the following subject areas: Art, Art History, any foreign language (German, Spanish or French at GRCC), History, Humanities, Literature, Music, Philosophy (but not Logic), or Theatre.						
	Cultural Enrichment Elective		3			
	Cultural Enrichment Elective		3			
	Cultural Enrichment Elective (200 level or above)		3			
Social Awareness – 9 Credits Required Subject areas include: Anthropology, Economics, Geography (but not Physical Geography; this course is considered a science elective), Political Science, Psychology or Sociology. Criteria: (1) One three-credit course must be 200-level or higher. (2) Must have two subject areas.						
	Social Awareness Elective		3			
	Social Awareness Elective		3			
	Social Awareness Elective (200 level or above)		3			
40-41 General Education Hours Required						

The University requires that one or more general education courses meet the **Global Consciousness and Race, Ethnicity and Gender (REG)** criteria. Students can take one course that meets both the Global and REG requirement simultaneously. Examples of GRCC or FSU courses that meet these criteria include:

Global and REG Courses Under Social Awareness:

ANTH 122 (AN 210 at GRCC) – Introduction to Cultural Anthropology
 GEOG 100 (GE 135 at GRCC) – Geography of World Regions
 GEOG 112 (GE 210 at GRCC) – Cultural Geography
 PLSC 323 – International Organization
 PLSC 331 (PS 201 at GRCC) – Comparative World Governments
 PLSC 341 (PS 202 at GRCC) – International Relations
 SOCY 335 (SO 270 at GRCC) – Marriage and the Family
 FSU PLSC Courses are taught in Grand Rapids primarily during the Summer Semester.

REG Courses Under Cultural Enrichment:

EN 270 (at GRCC) – Multicultural Literature
 LITR 202 (EN 271 at GRCC) – Black Literature
 PO 103 (at GRCC) – Introduction to Photography

Global Courses Under Cultural Enrichment:

Any foreign language course from GRCC
 HIST 152 (HS 102 at GRCC) – Western Civilization Since 1500
 HIST 373 (HS 290 at GRCC) – Twentieth Century Russia
 MUSI 232 (MU 107 at GRCC) – Introduction to Music Listening
 Note: MU 107 transfers into FSU as a 200-level course

REG Courses Under Social Awareness:

ANTH 121 (AN201 and 205 at GRCC) – Intro to Anthropology/Archaeology
 PLSC 121 (PS 110 at GRCC) – American Government 1
 PSYC 150 (PY 201 at GRCC) – Introduction to Psychology
 PSYC 226 (PY 232 at GRCC) – Lifespan Human Development
 PSYC 341 (PY 233 at GRCC) – Child Psychology
 PSYC 342 (PY 234 at GRCC) – Psychology of Adolescence
 SOCY 121 (SO 251 at GRCC) – Introductory Sociology
 SOCY 122 (SO 254 at GRCC) – Social Problems
 SOCY 340 (SO 260 at GRCC) – Minority Groups in America

Updated: August 31, 2011

Effective: Fall 2011 Semester

Advising Notes:

Global consciousness requirement satisfied by: _____

Race/Ethnicity/Gender requirement satisfied by: _____

Admission Requirements:

1. High school students must have a 3.0 cumulative GPA (on a 4.00 scale) and an ACT composite score of 22. College students must have a 2.70 cumulative GPA to be admitted to this program.
2. Apply online at www.ferris.edu/offcampus and submit official high school or college transcripts and ACT scores to Ferris State University, Office of admissions and records, 1201 Campus Drive CSS201, Big Rapids, MI. 49307-2288
3. Admission to GRCC College is also essential since many courses in the degree are completed through GRCC as a dual enrolled student.
4. Financial aid is available when dually enrolled in classes at Ferris State University and GRCC College. All financial aid will only originate with FSU to cover costs at both institutions. For more information regarding the financial aid process contact the main campus Financial Aid Office at 231-591-2110. For general financial aid questions you can also go to finaid@ferris.edu or for community college consortium questions go to cnsrtfinaid@ferris.edu.

Graduation Requirements:

1. A minimum of 120 semester credits must be completed for graduation – 40 of which must be 300 level or higher.
2. A 2.0 cumulative GPA is required in the major, concentration and overall for completion of the ISI degree.
3. At least 30 FSU semester credits must be completed to fulfill FSU residency requirements.
4. Students must meet the University General Education Requirements (*Refer to GRCC guidance regarding meeting the Ferris General Education requirements and /or GRCC MACRAO requirements*).

For more information or answers to your questions, contact us at:

Phone: 616.451.4777 or 800.998.3425

Fax: 616.451.4740

E-mail: fsugr@ferris.edu

Ferris State University – Grand Rapids
151 Fountain Street NE
Grand Rapids, MI 49503

Ferris ISI Core Course Descriptions (3 credit classes)

HSCJ 202-Principles of Information Security

Students explore the concepts of information security from both historical and emerging perspectives. Topics include the capabilities and threats of technology to information security, computer crime, homeland security, as well as legal, ethical and professional issues. The history, nature, and extent of computer crime and the roles and responsibilities of the legal system will also be investigated.

HSCJ 310-Digital Forensics and Analysis

Students learn the fundamentals of digital evidence collection and analysis. Emphasis is on both the collection of digital evidence and on common analysis tasks. Students will utilize various digital forensic tools and techniques for collection and analysis of digital evidence.

HSCJ 315-Advanced Digital Forensics

Students explore advanced digital forensic techniques and develop skills to deal with situations requiring a sophisticated response. Emerging and next generation computer technologies and threats, as well as proactive security measures and threat prevention will also be investigated. Students will utilize several digital forensic tools and techniques for collection, analysis, and incident processing.

HSCJ 317-Fraud Examination

Students will examine the fundamental reasons of why people commit fraud. Participants will investigate and explore how opportunity, pressures and rationalization are linked together to foster an atmosphere that can allow fraud to occur. Additionally, students will learn basic examination techniques for discovering fraud and more importantly, how to deter fraud from taking place.

ISIN 200-All Things Digital

Students investigate various digital devices including computers, cameras, surveillance equipment, and small devices and how to utilize them to advance security objectives. Students also work with various forms of media to understand the capabilities of each. Communication methods and networking are also explored.

ISIN 300-Visual Analysis Investigations

Introduction to transforming information into a visual format for analysis, interpretation and reporting. Students learn to deal with investigative issues involved to gather information, digital implications and strategies for effectively dealing with data from multiple sources. Analysis of digital data such as phone and financial records, surveillance information and visual media.

ISIN 301-Data-intelligence Comp Theory

Students examine the scientific process as it applies to hypothesis development. Investigation includes the analysis of various approaches to explaining events and developing competing hypothesis. The role of data and information in the development and support of intelligence in organization, national and international realms is also studied.

ISIN 312-Applications of Information Security

Students apply the tools and concepts of information security to mitigate and respond to risks. The theory and operation of information security tools and techniques are discussed, and students design and test their application in a variety of scenarios. Topics include software-, hardware-, host-, and network-based solutions.

ISIN 390-Special Topics in ISIN

This course covers various topics taught by diverse faculty.

ISIN 429-Legal-Ethical Issues Information Security

This course is intended to investigate the legal and ethical issues in Information Security. Ethical practices, privacy, copyright and licensing issues are research. Issues dealing with proprietary and personal information, as well as electronic technologies will be studied. An understanding of current and future impact on information systems and management strategies will be explored.

ISIN 499-Capstone Experience

This course provides students with an opportunity to demonstrate the skills and knowledge they have obtained in their program through project and/or portfolio methodologies and how they would be utilized in the workplace. Students will also investigate how information security is incorporated in their chosen path.

ISYS 371-Adv. Database Design and Implementation

Emphasis is placed on Entity-Relationships and Relational models, data definition languages, and manipulation languages. Structured Query Language (SQL) is used to develop database objects such as databases, logs, tables, indexes, views, constraints, defaults, roles, rules, stored procedures, and triggers. Database design is reviewed. Application development and modeling tools are discussed. Projects requiring the development of integrated databases are assigned.

PROJ 320-Project Management

An in-depth study of project management techniques currently employed for business and information systems projects. Topical areas will include project organization, planning and administration control and leadership. The need for accurate estimating, scheduling, communicating and reporting will be stressed through the use of several cases/projects. Senior Status

STQM 360-Risk Analysis and Strategy

Introduction to risk analysis and strategic approaches, principles, practices, tools, technology, and software. Risk analysis tools and approaches (e.g. planning, structured risk assessment, research and information discovery, probability and expectation, prioritization). Risk strategies, disposition, decision support, human resource development/management, and improvement/change strategies and tools. Application of risk analysis software. Applications and case studies to industry-specific events and projects (e.g. sport entertainment, security).

STQM 270-Introduction to Data Mining

Explore the relationship between data mining, data warehousing, and organizational needs. Explore basic data mining processes, methods and tools in varied areas of application such as business, manufacturing, healthcare, education, criminal justice, or government. Explore knowledge requirements across varied application areas as well as robust data mining processes and tools to serve varied needs. Case studies illustrate varied knowledge needs and data mining processes, methods, and tools. Introduces basic data mining software (e.g. WEKA, Excel based, or SPSS based).

Bachelor of Science

INFORMATION SECURITY & INTELLIGENCE

Lansing Community College – Transfer Guide (Effective Fall 2011)

As the only program of its kind in the country, Ferris Information Security & Intelligence (ISI) Program is at the forefront in its response to the need for skilled workers in Information Security/Data Analysis/Digital Investigation and Forensics. Developed with input from the U.S. Department of Homeland Security, the Pentagon, and investigative agencies; providing hands on utilization of state of the art technology, this program is uniquely positioned to satisfy the education credential necessary for students to be licensed as Professional Investigators in the State of Michigan, while our computer forensics coursework is accepted for meeting the education requirement to site for computer forensic examinations. In June 2011, Ferris State University formally received its designation as National Center of Academic Excellence in IA Education (CAE/IAE) by the NSA (National Security Agency), DOD (Department of Defense) and the DHS (Department of Homeland Security). Ferris successfully mapped its ISI (Information Security & Intelligence) and ISM (Information System Management) programs against all six NSA standards making it one of very few universities in the country to have achieved that level of mapping and the CAE/IAE designation.

General Admission Criteria

To be admitted to this program you must have a high school cumulative GPA of 3.0 and an ACT score of 22, or a 2.7 cumulative GPA as a transfer student. You will need to submit official transcripts from all colleges/universities with your application.

Course Requirements

Lansing Community College

(FSU equivalences are in parentheses)

General Education Requirements (satisfied by MACRAO Stamp)

SPCH 140 Interpersonal Communication (COMM 105) or	
SPCH 130 Fundamentals Public Speaking (COMM 121).....	3
WRIT 121 Composition 1 (ENG 150)	3
WRIT 127 Business Writing (ENG 211)	3
Scientific Understanding w/Lab.....	4
Scientific Understanding without Lab.....	3
Cultural Enrichment Electives.....	9
Social Awareness Electives.....	9
MATH 112 Intermediate Algebra (MATH 115)	3
(Students must satisfy Global Consciousness & Race, Ethnicity, Gender requirements if they do not receive a MACRAO stamp)	

Business Core Courses

MGMT 335 Managerial Statistics (STQM 260).....	3
ACCG 210 Principles of Accounting 1 (ACT 201).....	4
MGMT 225 Principles of Mgmt/Leadership or	
MGMT 300 Leadership (MGMT 301).....	3
MKTG 200 Principles of Marketing (MKTG 321).....	3

Ferris State University

General Education Courses

ENG 311 or 321 or 325 Advanced Writing.....	3
---	---

Business Core Courses

MGMT 350 Tools for Decision Making	3
--	---

Information Security & Intelligence Major Core

STQM 270 Introduction to Data Mining.....	3
STQM 360 Risk Analysis and Strategy.....	3
ISIN 200 All Things Digital.....	3
HSCJ 202 Principles of Information Security	3
HSCJ 310 Digital Forensics and Incident Response.....	3
PROJ 320 Project Management Fundamentals	3
HSCJ 317 Fraud Examination.....	3
ISIN 429 Legal and Ethical Issues in Security	3
ISIN 300 Visual Analysis.....	3
ISYS 200 Database Design (CITD 250).....	3
ISIN 301 Data Intelligence Competitive Theory.....	3

ISIN 312 Applications of Information Security	3
ISIN 390 Special Topics in Information Security.....	3
ISIN 491 Intership.....	3
ISIN 499 Capstone (Senior Standing).....	3
Directed Electives	7

Available ISI Concentrations

Ferris State University (LCC courses in parenthesis)

Digital Forensics

HSCJ 315 Advanced Digital Forensics	3
ISYS 216 Java (CITP 190).....	3
ISYS 325 Networking Essentials (CITN 220).....	3
ISYS 371 Advanced Database	3

Network Security

ISYS 277 Linux Network Administration (CITN 230)	3
ISYS 325 Networking Essentials (CITN 220).....	3
Approved Elective	3
Approved Elective	3

Project Management (Online)

PROJ 350 Project Scheduling	3
ISYS 351 Project Communication	3
PROJ 420 Project Procurement & PMP Prep.....	3
MGMT 370 Quality Operations Management	3

Foreign Language

Foreign Language Classes.....	12
-------------------------------	----

Total Gen Ed Credits	40
Total Business Core Credits	16
Total ISI Core Credits.....	45
Total Concentration Credits.....	12
Directed Electives Credits.....	7
TOTAL CREDITS	120

For more information, call or visit us online.

1.800.998.3425 or 1.616.451.4777

www.ferris.edu/Statewide

Ferris State University
B.S. Degree in Information Security & Intelligence

*** Effective Fall 2012 ***

Lansing Community College

Student Checksheet

NAME: _____ ID#: _____ DATE _____ ADVISOR: _____

Major Core Requirements (60 credits): LCC College equivalent courses are identified in third column. **FSU classes are in bold.**
 Highlighted courses are available online.

Required Courses	Course Title– FSU Prerequisites Shown in Parentheses ()	LCC Equivalent Courses	FSU S. H.	Planned	Completed	Grade
ACCT 201	Principles of Accounting (MATH 110 w/C- or better or 19 on ACT or 460 on SAT or one of the following MATH courses 115 to 120, 126, 130, 132, 135)	ACCG 210	3			
MGMT 301	Applied Management	MGMT 225 or MGMT 300	3			
MKTG 321	Principles of Marketing (sophomore status or instructor permit)	MKTG 200	3			
MGMT 350	Tools for Decision Making	FSU class	3			
STQM 260	Introduction to Statistics (MATH 115, 116 or 117 or 24 ACT or 560 SAT)	MGMT 335	3			
STQM 270	Introduction to Data Mining (STQM 260)	FSU class	3			
STQM 360	Risk Analysis and Strategy (STQM 260)	FSU class	3			
ISYS 200	Database Design & Implementation (ISYS 105 or demonstrated competency)	CITD 250	3			
PROJ 320	Project Management	FSU class	3			
HSCJ 202	Principles of Information Security	FSU class				
HSCJ 310	Digital Forensics and Analysis (HSCJ 202)	FSU class	3			
HSCJ 317	Fraud Examination	FSU class	3			
ISIN 200	All Things Digital	FSU class	3			
ISIN 300	Visual Analysis and Investigations	FSU class	3			
ISIN 301	Data Intelligence Competitive Theory (ISIN 300, ISYS 200)	FSU class	3			
ISIN312	Applications of Information Security (HSCJ 202)	FSU class	3			
ISIN 390	Special Topics in ISIN	FSU class	3			
ISIN 429	Legal & Ethical Issues in Information Security	FSU class	3			
ISIN 491	Internship	FSU class	3			
ISIN 499	Capstone Experience (Senior Standing)	FSU class	3			
	Total					
	Major Core Credits Required: 60 credits					
	Directed Electives: 7-8 Credits Required (to total 120 credits for the BS Degree)					
	Note: Discuss with Advisor - 300-400 level classes may be needed here to fulfill the 40 credit 300-400 level requirements in the degree					
		FSU or LCC	3			
		FSU or LCC	3			
		FSU or LCC	1-2			

Concentration or an approved minor (12 Credits Required)						
Digital Forensics						
HSCJ 315	Advanced Digital Forensics (HSCJ 310)	FSU Class	3			
ISYS 216	Intro to Java Programming (ISYS 110)	CITP 190	3			
ISYS 371	Advanced Database Design & Implementation (ISYS 200 & ISYS 216)		3			
ISYS 325	Networking Essentials (ISYS 105 or demonstrated competency)	<i>CITN 220</i>	3			
GIS						
GISC 225	Principles of GIS	Ferris class	3			
GISC 282	Geographic Information Systems 2	Ferris class	3			
GISC 382	GIS Data Analysis	Ferris class	3			
ISYS 371	Adv Database Design-Implement		3			
Network Security						
ISYS 277	Linux Network Administration	CITN 230	3			
ISYS 325	Networking Essentials (ISYS 105 or demonstrated competency)	CITN 220	3			
	Elective		3			
	Elective		3			
Project Management (Online)						
PROJ 350	Project Schedule, Cost and Risk Management	Ferris class	3			
PROJ 351	Project Communication, Team Building and Conflict Management	Ferris class	3			
PROJ 420	Managing the Procurement Process and Preparing for the PMP	Ferris class	3			
MGMT 370	Quality-Operations Management	Ferris class	3			
Foreign Language						
	Foreign Language 1		3			
	Foreign Language 2		3			
	Foreign Language 3		3			
	Foreign Language 4		3			

Updated: August 31, 2011
Effective: Fall 2011 Semester

General Education Requirements (40-41 Credits):

EARNED MACRAO STAMP: YES NO

Required Courses	Course Title FSU Prerequisites Shown in Parentheses ()	LCC Equivalent Courses	FSU S.H.	Planned	Completed	Grade
Communication Competence—12 Credits Required						
COMM ELEC	COMM 105, Interpersonal Communication or COMM 121, Fundamentals of Public Speaking	SPCH 140 or SPCH 130	3			
ENGL 150	English 1 (ENGL 074 w/C- or better or 14 > ACT or 370 > SAT)	WRIT 121	3			
ENGL 211 or ENGL 250	Industrial and Career Writing (ENGL 150 w/C- or better) English 2 (ENGL 150 w/C- or better)	WRIT 127	3			
ENGL 311 or ENGL 321 or ENGL 325	Advanced Technical Writing (ENGL 250 or ENGL 211 w/C or better) Advanced Composition (ENGL 250 or ENGL 211 w/C or better) Advanced Business Writing (ENGL 250 or ENGL 211 w/C or better)	FSU Class	3			
Scientific Understanding – 7 to 8 Credits Required This requirement can be met with science courses in the following areas: Astronomy, Biology, Chemistry, Geology, Physical Science, Physics, or FSU's GEOG 111 or GEOG 121						
	Scientific Understanding Elective with Lab		4			
	Scientific Understanding Elective (Lab or Non-Lab)		3 or 4			
Quantitative Skills – This requirement can be completed by one of the following options: (1) pass Math 115 or higher, (2) pass course proficiency exam in Math 115 or higher, (3) pass the College Algebra CLEP exam, or (4) an ACT math subtest score of 24 or higher.						
MATH 115	Intermediate Algebra (ACT of 19-21 or SAT of 350- 450)	MAT 112	3			
Cultural Enrichment – 9 Credits Required Credits can be earned in one or more subject areas; however, one three-credit course must be at the 200 level or higher. Select from the following subject areas: Art, Art History, any foreign language (German, Spanish or French at LCC), History, Humanities, Literature, Music, Philosophy (but not Logic), or Theatre.						
	Cultural Enrichment Elective		3			
	Cultural Enrichment Elective		3			
	Cultural Enrichment Elective (200 level or above)		3			
Social Awareness – 9 Credits Required Subject areas include: Anthropology, Economics, Geography (but not Physical Geography; this course is considered a science elective), Political Science, Psychology or Sociology. Criteria: (1) One three-credit course must be 200-level or higher. (2) Must have two subject areas.						
	Social Awareness Elective		3			
	Social Awareness Elective		3			
	Social Awareness Elective (200 level or above)		3			
40-41 General Education Hours Required						

Advising Notes:

Global consciousness requirement satisfied by: _____
Race/Ethnicity/Gender requirement satisfied by: _____

Admission Requirements:

1. High school students must have a 3.0 cumulative GPA (on a 4.00 scale) and an ACT composite score of 22. College students must have a 2.70 cumulative GPA to be admitted to this program.
2. Apply online at www.ferris.edu/offcampus and submit official high school or college transcripts and ACT scores to Ferris State University, Office of admissions and records, 1201 Campus Drive CSS201, Big Rapids, MI. 49307-2288
3. Admission to LCC College is also essential since many courses in the degree are completed through LCC as a dual enrolled student.
4. Financial aid is available when dually enrolled in classes at Ferris State University and LCC College. All financial aid will only originate with FSU to cover costs at both institutions. For more information regarding the financial aid process contact the main campus Financial Aid Office

Updated: August 31, 2011
Effective: Fall 2011 Semester

at 231-591-2110. For general financial aid questions you can also go to finaid@ferris.edu or for community college consortium questions go to cnsrtfinaid@ferris.edu.

Graduation Requirements:

1. A minimum of 120 semester credits must be completed for graduation – 40 of which must be 300 level or higher.
2. A 2.0 cumulative GPA is required in the major, concentration and overall for completion of the ISI degree.
3. At least 30 FSU semester credits must be completed to fulfill FSU residency requirements.
4. Students must meet the University General Education Requirements (*Refer to LCC guidance regarding meeting the Ferris General Education requirements and /or LCC MACRAO requirements*).

Ferris ISI Core Course Descriptions (3 credit classes)

HSCJ 202-Principles of Information Security

Students explore the concepts of information security from both historical and emerging perspectives. Topics include the capabilities and threats of technology to information security, computer crime, homeland security, as well as legal, ethical and professional issues. The history, nature, and extent of computer crime and the roles and responsibilities of the legal system will also be investigated.

HSCJ 310-Digital Forensics and Analysis

Students learn the fundamentals of digital evidence collection and analysis. Emphasis is on both the collection of digital evidence and on common analysis tasks. Students will utilize various digital forensic tools and techniques for collection and analysis of digital evidence.

HSCJ 315-Advanced Digital Forensics

Students explore advanced digital forensic techniques and develop skills to deal with situations requiring a sophisticated response. Emerging and next generation computer technologies and threats, as well as proactive security measures and threat prevention will also be investigated. Students will utilize several digital forensic tools and techniques for collection, analysis, and incident processing.

HSCJ 317-Fraud Examination

Students will examine the fundamental reasons of why people commit fraud. Participants will investigate and explore how opportunity, pressures and rationalization are linked together to foster an atmosphere that can allow fraud to occur. Additionally, students will learn basic examination techniques for discovering fraud and more importantly, how to deter fraud from taking place.

ISIN 200-All Things Digital

Students investigate various digital devices including computers, cameras, surveillance equipment, and small devices and how to utilize them to advance security objectives. Students also work with various forms of media to understand the capabilities of each. Communication methods and networking are also explored.

ISIN 300-Visual Analysis Investigations

Introduction to transforming information into a visual format for analysis, interpretation and reporting. Students learn to deal with investigative issues involved to gather information, digital implications and strategies for effectively dealing with data from multiple sources. Analysis of digital data such as phone and financial records, surveillance information and visual media.

ISIN 301-Data-intelligence Comp Theory

Students examine the scientific process as it applies to hypothesis development. Investigation includes the analysis of various approaches to explaining events and developing competing hypothesis. The role of data and information in the development and support of intelligence in organization, national and international realms is also studied.

ISIN 312-Applications of Information Security

Students apply the tools and concepts of information security to mitigate and respond to risks. The theory and operation of information security tools and techniques are discussed, and students design and test their application in a variety of scenarios. Topics include software-, hardware-, host-, and network-based solutions.

ISIN 390-Special Topics in ISIN

This course covers various topics taught by diverse faculty.

ISIN 429-Legal-Ethical Issues Information Security

This course is intended to investigate the legal and ethical issues in Information Security. Ethical practices, privacy, copyright and licensing issues are research. Issues dealing with proprietary and personal information, as well as electronic technologies will be studied. An understanding of current and future impact on information systems and management strategies will be explored.

ISIN 499-Capstone Experience

This course provides students with an opportunity to demonstrate the skills and knowledge they have obtained in their program through project and/or portfolio methodologies and how they would be utilized in the workplace. Students will also investigate how information security is incorporated in their chosen path.

ISYS 371-Adv. Database Design and Implementation

Emphasis is placed on Entity-Relationships and Relational models, data definition languages, and manipulation languages. Structured Query Language (SQL) is used to develop database objects such as databases, logs, tables, indexes, views, constraints, defaults, roles, rules, stored procedures, and triggers. Database design is reviewed. Application development and modeling tools are discussed. Projects requiring the development of integrated databases are assigned.

PROJ 320-Project Management

An in-depth study of project management techniques currently employed for business and information systems projects. Topical areas will include project organization, planning and administration control and leadership. The need for accurate estimating, scheduling, communicating and reporting will be stressed through the use of several cases/projects. Senior Status

STQM 360-Risk Analysis and Strategy

Introduction to risk analysis and strategic approaches, principles, practices, tools, technology, and software. Risk analysis tools and approaches (e.g. planning, structured risk assessment, research and information discovery, probability and expectation, prioritization). Risk strategies, disposition, decision support, human resource development/management, and improvement/change strategies and tools. Application of risk analysis software. Applications and case studies to industry-specific events and projects (e.g. sport entertainment, security).

STQM 270-Introduction to Data Mining

Explore the relationship between data mining, data warehousing, and organizational needs. Explore basic data mining processes, methods and tools in varied areas of application such as business, manufacturing, healthcare, education, criminal justice, or government. Explore knowledge requirements across varied application areas as well as robust data mining processes and tools to serve varied needs. Case studies illustrate varied knowledge needs and data mining processes, methods, and tools. Introduces basic data mining software (e.g. WEKA, Excel based, or SPSS based).



Bachelor of Science

INFORMATION SECURITY & INTELLIGENCE

Northwestern Michigan College – Transfer Guide

As the only program of its kind in the country, Ferris Information Security & Intelligence (ISI) Program is at the forefront in its response to the need for skilled workers in Information Security/Data Analysis/Digital Investigation and Forensics. Developed with input from the U.S. Department of Homeland Security, the Pentagon, and investigative agencies; providing hands on utilization of state of the art technology, this program is uniquely positioned to satisfy the education credential necessary for students to be licensed as Professional Investigators in the State of Michigan, while our computer forensics coursework is accepted for meeting the education requirement to site for computer forensic examinations. In June 2011, Ferris State University formally received its designation as National Center of Academic Excellence in IA Education (CAE/IAE) by the NSA (National Security Agency) and the DHS (Department of Homeland Security). Ferris successfully mapped its ISI (Information Security & Intelligence) and ISM (Information System Management) programs classes against all six NSA standards making it one of very few universities in the country to have achieved that level of mapping and the CAE/IAE designation.

General Admission Criteria

To be admitted to this program you must have a high school cumulative GPA of 3.0 and an ACT score of 22, or a 2.7 cumulative GPA as a transfer student. You will need to submit official transcripts from all colleges/university with your application.

Course Requirements

Northwestern Michigan College

General Education Requirements (satisfied by MACRAO Stamp)

COM111 Speech (COMM 121).....	3
ENG 111 Composition 1 (ENG 150).....	3
ENG 112 Composition 2 (ENG 250).....	3
Scientific Understanding w/Lab.....	4
Scientific Understanding without Lab.....	3
Cultural Enrichment Electives (9 credits).....	9
Social Awareness Electives (9 credits).....	9
MATH 111 Intermediate Algebra (MATH 115).....	3
(Students must satisfy Global Consciousness & Race, Ethnicity, Gender requirements if they do not receive a MACRAO stamp)	

Business Core Courses

MTH 131 Statistics (STQM 260).....	3
ACC 121 Principles of Accounting (ACT 201).....	4
MGT 241 Applied Management (MGMT 301).....	3
MKT 201 Principles of Marketing (MKTG 321).....	3

Ferris State University (NMC courses in parenthesis)

General Education Courses

ENG 311 or 321 or 325 Advanced Writing.....	3
---	---

Business Core Courses

MGMT 350 Tools for Decision Making.....	3
---	---

Information Security & Intelligence Major Core

STQM 270 Introduction to Data Mining.....	3
STQM 360 Risk Analysis and Strategy.....	3
ISIN 200 All Things Digital.....	3
HSCJ 202 Principles of Information Security.....	3
HSCJ 310 Digital Forensics and Incident Response.....	3
PROJ 320 Project Management Fundamentals.....	3
HSCJ 317 Fraud Examination.....	3
ISIN 429 Legal and Ethical Issues in Security.....	3
ISIN 300 Visual Analysis.....	3
ISYS 200 Database Design (CIT 212).....	3
ISIN 301 Data Intelligence Competitive Theory.....	3

ISIN 312 Applications of Information Security.....	3
ISIN 390 Special Topics in Information Security.....	3
ISIN 491 Internship.....	3
ISIN 499 Capstone (Senior Standing).....	3
Directed Electives.....	7

Available ISI Concentrations

Ferris State University (NMC courses in parenthesis)

Digital Forensics

HSCJ 315 Advanced Digital Forensics.....	3
ISYS 216 Java (CIT 255).....	3
ISYS 325 Networking Essentials (CIT 213).....	3
ISYS 371 Advanced Database (CIT 248).....	3

Network Security

ISYS 277 Linux Network Administration (CIT256).....	3
ISYS 325 Networking Essentials (CIT 213).....	3
Approved Elective.....	3
Approved Elective.....	3

Project Management (Online)

PROJ 350 Project Scheduling.....	3
ISYS 351 Project Communication.....	3
PROJ 420 Project Procurement & PMP Prep.....	3
MGMT 370 Quality Operations Management.....	3

Foreign Language

Foreign Language Classes.....	12
-------------------------------	----

Total Gen Ed Credits.....	40
Total Business Core Credits.....	16
Total ISI Core Credits.....	45
Total Concentration Credits.....	12
Directed Electives Credits.....	7
TOTAL CREDITS.....	120

For more information, call or visit us online.

1.800.998.3425 or 1.616.451.4777

www.ferris.edu/Statewide

Ferris State University
B.S. Degree in Information Security & Intelligence

*** Effective Fall 2011 ***

Northwestern Michigan College

Student Checksheet

NAME: _____ ID#: _____ DATE _____ ADVISOR: _____

Major Core Requirements (60 credits): NMC College equivalent courses are identified in third column. **FSU classes are in bold.**
 Highlighted courses are available online.

Required Courses	Course Title– FSU Prerequisites Shown in Parentheses ()	NMC Equivalent Courses	FSU S. H.	Planned	Completed	Grade
ACCT 201	Principles of Accounting (MATH 110 w/C- or better or 19 on ACT or 460 on SAT or one of the following MATH courses 115 to 120, 126, 130, 132, 135)	ACC 121	3			
MGMT 301	Applied Management	MGT 241	3			
MKTG 321	Principles of Marketing (sophomore status or instructor permit)	MKT 201	3			
MGMT 350	Tools for Decision Making	FSU class	3			
STQM 260	Introduction to Statistics (MATH 115, 116 or 117 or 24 ACT or 560 SAT)	MTH 131	3			
STQM 270	Introduction to Data Mining (STQM 260)	FSU class	3			
STQM 360	Risk Analysis and Strategy (STQM 260)	FSU class	3			
ISYS 200	Database Design & Implementation (ISYS 105 or demonstrated competency)	CIT 212	3			
PROJ 320	Project Management	FSU class	3			
HSCJ 202	Principles of Information Security	FSU class				
HSCJ 310	Digital Forensics and Analysis (HSCJ 202)	FSU class	3			
HSCJ 317	Fraud Examination	FSU class	3			
ISIN 200	All Things Digital	FSU class	3			
ISIN 300	Visual Analysis and Investigations	FSU class	3			
ISIN 301	Data Intelligence Competitive Theory (ISIN 300, ISYS 200)	FSU class	3			
ISIN312	Applications of Information Security (HSCJ 202)	FSU class	3			
ISIN 390	Special Topics in ISIN	FSU class	3			
ISIN 429	Legal & Ethical Issues in Information Security	FSU class	3			
ISIN 491	Internship	FSU class	3			
ISIN 499	Capstone Experience (Senior Standing)	FSU class	3			
	Total					
	Major Core Credits Required: 60 credits					
	Directed Electives: 7-8 Credits Required (to total 120 credits for the BS Degree)					
	Note: Discuss with Advisor - 300-400 level classes may be needed here to fulfill the 40 credit 300-400 level requirements in the degree					
		FSU or NMC	3			
		FSU or NMC	3			
		FSU or NMC	1-2			

Concentration or an approved minor (12 Credits Required						
Digital Forensics						
HSCJ 315	Advanced Digital Forensics (HSCJ 310)	FSU Class	3			
ISYS 216	Intro to Java Programming (ISYS 110)	CIT 255	3			
ISYS 371	Advanced Database Design & Implementation (ISYS 200 & ISYS 216)	CIT 248	3			
ISYS 325	Networking Essentials (ISYS 105 or demonstrated competency)	CIT 213	3			
Network Security						
ISYS 277	Linux Network Administration	CIT 256	3			
ISYS 325	Networking Essentials (ISYS 105 or demonstrated competency)	CIT 213	3			
	Elective		3			
	Elective		3			
Project Management (Online)						
PROJ 350	Project Schedule, Cost and Risk Management	Ferris class	3			
PROJ 351	Project Communication, Team Building and Conflict Management	Ferris class	3			
PROJ 420	Managing the Procurement Process and Preparing for the PMP	Ferris class	3			
MGMT 370	Quality-Operations Management	Ferris class	3			
Foreign Language						
	Foreign Language 1		3			
	Foreign Language 2		3			
	Foreign Language 3		3			
	Foreign Language 4		3			

Updated: August 31, 2011
Effective: Fall 2011 Semester

General Education Requirements (40-41 Credits):

EARNED MACRAO STAMP: YES NO

Required Courses	Course Title FSU Prerequisites Shown in Parentheses ()	NMC Equivalent Courses	FSU S.H.	Planned	Completed	Grade
Communication Competence—12 Credits Required						
COMM ELEC	COMM 105, Interpersonal Communication or COMM 121, Fundamentals of Public Speaking	COM 111	3			
ENGL 150	English 1 (ENGL 074 w/C- or better or 14 > ACT or 370 > SAT)	ENG 111	3			
ENGL 211 or ENGL 250	Industrial and Career Writing (ENGL 150 w/C- or better) English 2 (ENGL 150 w/C- or better)	ENG 112	3			
ENGL 311 or ENGL 321 or ENGL 325	Advanced Technical Writing (ENGL 250 or ENGL 211 w/C or better) Advanced Composition (ENGL 250 or ENGL 211 w/C or better) Advanced Business Writing (ENGL 250 or ENGL 211 w/C or better)	FSU Class	3			
Scientific Understanding – 7 to 8 Credits Required						
This requirement can be met with science courses in the following areas: Astronomy, Biology, Chemistry, Geology, Physical Science, Physics, or FSU's GEOG 111 or GEOG 121						
	Scientific Understanding Elective with Lab		4			
	Scientific Understanding Elective (Lab or Non-Lab)		3 or 4			
Quantitative Skills – This requirement can be completed by one of the following options: (1) pass Math 115 or higher, (2) pass course proficiency exam in Math 115 or higher, (3) pass the College Algebra CLEP exam, or (4) an ACT math subtest score of 24 or higher.						
MATH 115	Intermediate Algebra (ACT of 19-21 or SAT of 350- 450)	MAT 111	3			
Cultural Enrichment – 9 Credits Required						
Credits can be earned in one or more subject areas; however, one three-credit course must be at the 200 level or higher. Select from the following subject areas: Art, Art History, any foreign language (German, Spanish or French at NMC), History, Humanities, Literature, Music, Philosophy (but not Logic), or Theatre.						
	Cultural Enrichment Elective	NMC or MACROA	3			
	Cultural Enrichment Elective	NMC or MACROA	3			
	Cultural Enrichment Elective (200 level or above)	NMC or MACROA	3			
Social Awareness – 9 Credits Required						
Subject areas include: Anthropology, Economics, Geography (but not Physical Geography; this course is considered a science elective), Political Science, Psychology or Sociology. Criteria: (1) One three-credit course must be 200-level or higher. (2) Must have two subject areas.						
	Social Awareness Elective	NMC or MACROA	3			
	Social Awareness Elective	NMC or MACROA	3			
	Social Awareness Elective (200 level or above)	NMC or MACROA	3			
40-41 General Education Hours Required						

Advising Notes:

Global consciousness requirement satisfied by: _____

Race/Ethnicity/Gender requirement satisfied by: _____

Admission Requirements:

1. High school students must have a 3.0 cumulative GPA (on a 4.00 scale) and an ACT composite score of 22. College students must have a 2.70 cumulative GPA to be admitted to this program.
2. Apply online at www.ferris.edu/offcampus and submit official high school or college transcripts and ACT scores to Ferris State University, Office of admissions and records, 1201 Campus Drive CSS201, Big Rapids, MI. 49307-2288
3. Admission to NMC College is also essential since many courses in the degree are completed through NMC as a dual enrolled student.
4. Financial aid is available when dually enrolled in classes at Ferris State University and NMC College. All financial aid will only originate with FSU to cover costs at both institutions. For more information regarding the financial aid process contact the main campus Financial Aid Office

Updated: August 31, 2011

Effective: Fall 2011 Semester

at 231-591-2110. For general financial aid questions you can also go to finaid@ferris.edu or for community college consortium questions go to cnsrtfinaid@ferris.edu.

Graduation Requirements:

1. A minimum of 120 semester credits must be completed for graduation – 40 of which must be 300 level or higher.
2. A 2.0 cumulative GPA is required in the major, concentration and overall for completion of the ISI degree.
3. At least 30 FSU semester credits must be completed to fulfill FSU residency requirements.
4. Students must meet the University General Education Requirements (*Refer to NMC guidance regarding meeting the Ferris General Education requirements and /or NMC MACRAO requirements*).

Ferris ISI Core Course Descriptions (3 credit classes)

HSCJ 202-Principles of Information Security

Students explore the concepts of information security from both historical and emerging perspectives. Topics include the capabilities and threats of technology to information security, computer crime, homeland security, as well as legal, ethical and professional issues. The history, nature, and extent of computer crime and the roles and responsibilities of the legal system will also be investigated.

HSCJ 310-Digital Forensics and Analysis

Students learn the fundamentals of digital evidence collection and analysis. Emphasis is on both the collection of digital evidence and on common analysis tasks. Students will utilize various digital forensic tools and techniques for collection and analysis of digital evidence.

HSCJ 315-Advanced Digital Forensics

Students explore advanced digital forensic techniques and develop skills to deal with situations requiring a sophisticated response. Emerging and next generation computer technologies and threats, as well as proactive security measures and threat prevention will also be investigated. Students will utilize several digital forensic tools and techniques for collection, analysis, and incident processing.

HSCJ 317-Fraud Examination

Students will examine the fundamental reasons of why people commit fraud. Participants will investigate and explore how opportunity, pressures and rationalization are linked together to foster an atmosphere that can allow fraud to occur. Additionally, students will learn basic examination techniques for discovering fraud and more importantly, how to deter fraud from taking place.

ISIN 200-All Things Digital

Students investigate various digital devices including computers, cameras, surveillance equipment, and small devices and how to utilize them to advance security objectives. Students also work with various forms of media to understand the capabilities of each. Communication methods and networking are also explored.

ISIN 300-Visual Analysis Investigations

Introduction to transforming information into a visual format for analysis, interpretation and reporting. Students learn to deal with investigative issues involved to gather information, digital implications and strategies for effectively dealing with data from multiple sources. Analysis of digital data such as phone and financial records, surveillance information and visual media.

ISIN 301-Data-intelligence Comp Theory

Students examine the scientific process as it applies to hypothesis development. Investigation includes the analysis of various approaches to explaining events and developing competing hypothesis. The role of data and information in the development and support of intelligence in organization, national and international realms is also studied.

ISIN 312-Applications of Information Security

Students apply the tools and concepts of information security to mitigate and respond to risks. The theory and operation of information security tools and techniques are discussed, and students design and test their application in a variety of scenarios. Topics include software-, hardware-, host-, and network-based solutions.

ISIN 390-Special Topics in ISIN

This course covers various topics taught by diverse faculty.

ISIN 429-Legal-Ethical Issues Information Security

This course is intended to investigate the legal and ethical issues in Information Security. Ethical practices, privacy, copyright and licensing issues are research. Issues dealing with proprietary and personal information, as well as electronic technologies will be studied. An understanding of current and future impact on information systems and management strategies will be explored.

ISIN 499-Capstone Experience

This course provides students with an opportunity to demonstrate the skills and knowledge they have obtained in their program through project and/or portfolio methodologies and how they would be utilized in the workplace. Students will also investigate how information security is incorporated in their chosen path.

ISYS 371-Adv. Database Design and Implementation

Emphasis is placed on Entity-Relationships and Relational models, data definition languages, and manipulation languages. Structured Query Language (SQL) is used to develop database objects such as databases, logs, tables, indexes, views, constraints, defaults, roles, rules, stored procedures, and triggers. Database design is reviewed. Application development and modeling tools are discussed. Projects requiring the development of integrated databases are assigned.

PROJ 320-Project Management

An in-depth study of project management techniques currently employed for business and information systems projects. Topical areas will include project organization, planning and administration control and leadership. The need for accurate estimating, scheduling, communicating and reporting will be stressed through the use of several cases/projects. Senior Status

STQM 360-Risk Analysis and Strategy

Introduction to risk analysis and strategic approaches, principles, practices, tools, technology, and software. Risk analysis tools and approaches (e.g. planning, structured risk assessment, research and information discovery, probability and expectation, prioritization). Risk strategies, disposition, decision support, human resource development/management, and improvement/change strategies and tools. Application of risk analysis software. Applications and case studies to industry-specific events and projects (e.g. sport entertainment, security).

STQM 270-Introduction to Data Mining

Explore the relationship between data mining, data warehousing, and organizational needs. Explore basic data mining processes, methods and tools in varied areas of application such as business, manufacturing, healthcare, education, criminal justice, or government. Explore knowledge requirements across varied application areas as well as robust data mining processes and tools to serve varied needs. Case studies illustrate varied knowledge needs and data mining processes, methods, and tools. Introduces basic data mining software (e.g. WEKA, Excel based, or SPSS based).

Bachelor of Science

INFORMATION SECURITY & INTELLIGENCE

Wayne County Community College District – Transfer Guide

As the only program of its kind in the country, Ferris Information Security & Intelligence (ISI) Program is at the forefront in its response to the need for skilled workers in Information Security/Data Analysis/Digital Investigation and Forensics. Developed with input from the U.S. Department of Homeland Security, the Pentagon, and investigative agencies; providing hands on utilization of state of the art technology, this program is uniquely positioned to satisfy the education credential necessary for students to be licensed as Professional Investigators in the State of Michigan, while our computer forensics coursework is accepted for meeting the education requirement to site for computer forensic examinations. In June 2011, Ferris State University formally received its designation as National Center of Academic Excellence in IA Education (CAE/IAE) by the NSA (National Security Agency) and the DHS (Department of Homeland Security). Ferris successfully mapped its ISI (Information Security & Intelligence) and ISM (Information System Management) programs classes against all six NSA standards making it one of very few universities in the country to have achieved that level of mapping and the CAE/IAE designation.

General Admission Criteria

WCCCD students who have completed the Associate degree or have completed at least 48+ transfer credits from WCCCD with a cumulative gpa of not less than a 2.7 (on a 4.0 scale) or higher may apply to the B.S. degree program at FSU. WCCCD's definition of a Pass grade does not include the equivalent of a grade lower than a grade of C (or a 2.00 on a 4.00 scale).

Course Requirements

Wayne County Community College District (FSU equivalencies are in parentheses)

General Education Requirements (satisfied by MACRAO Stamp)

SPH 100 Interpersonal Communication (COMM 105) or SPH 101 Fundamentals of Speech (COMM 121).....	3
ENG 110 English 1 or 120 English 2 (ENG 150).....	3
ENG 270 Professional and Technical Writing (ENG 211).....	3
Scientific Understanding w/Lab.....	4
Scientific Understanding without Lab.....	3
Cultural Enrichment Electives.....	9
Social Awareness Electives.....	9
MATH 113 Intermediate Algebra (MATH 115).....	3
MATH 115 is not covered in the MACRAO agreement. Also, students must satisfy Global Consciousness & Race, Ethnicity, Gender requirements if they do not receive a MACRAO stamp)	

Business Core Courses

BUS 221 Business Statistics or MAT 131 Descriptive Statistics (STQM 260).....	3
ACC 110 Principles of Accounting 1 (ACT 201).....	4
MGT 205 Management Principles (MGMT 301).....	3
MKT 200 Principles of Marketing (MKTG 321).....	3

Ferris State University

General Education Courses

ENG 311 or 321 or 325 Advanced Writing.....	3
---	---

Business Core Courses

MGMT 350 Tools for Decision Making.....	3
---	---

Information Security & Intelligence Major Core

STQM 270 Introduction to Data Mining.....	3
STQM 360 Risk Analysis and Strategy.....	3
ISIN 200 All Things Digital.....	3
HSCJ 202 Principles of Information Security.....	3
HSCJ 310 Digital Forensics and Incident Response.....	3
PROJ 320 Project Management Fundamentals.....	3
HSCJ 317 Fraud Examination.....	3
ISIN 429 Legal and Ethical Issues in Security.....	3
ISIN 300 Visual Analysis.....	3
ISYS 200 Database Design (CIS 285).....	3
ISIN 301 Data Intelligence Competitive Theory.....	3
ISIN 312 Applications of Information Security.....	3
ISIN 390 Special Topics in Information Security.....	3
ISIN 491 Internship.....	3

ISIN 499 Capstone (Senior Standing).....	3
Directed Electives.....	7

Available ISI Concentrations

Ferris State University (WCCCD courses in parenthesis)

Digital Forensics

HSCJ 315 Advanced Digital Forensics.....	3
ISYS 216 Java (CIS 259 or CIS 207).....	3
ISYS 325 Networking Essentials (CIS 287).....	3
ISYS 371 Advanced Database (CIS 246).....	3

Network Security

ISYS 277 Linux Network Administration (CIS 240).....	3
ISYS 325 Networking Essentials (CIS 287).....	3
Approved Elective.....	3
Approved Elective.....	3

Project Management (Online)

PROJ 350 Project Scheduling.....	3
ISYS 351 Project Communication.....	3
PROJ 420 Project Procurement & PMP Prep.....	3
MGMT 370 Quality Operations Management.....	3

National Security (Online)

ISIN 350 Organizational Planning and Security Measures.....	3
ISIN 351 Global Security and Policy.....	3
ISIN 352 The Role of Intelligence.....	3
Approved Elective.....	3

Foreign Language

Foreign Language Classes.....	12
-------------------------------	----

Total Gen Ed Credits.....	40
Total Business Core Credits.....	16
Total ISI Core Credits.....	45
Total Concentration Credits.....	12
Directed Electives Credits.....	7
TOTAL CREDITS.....	120

For more information, call or visit us online.
1.800.998.3425 or 1.586.263.6773
www.ferris.edu/Statewide

Ferris State University
B.S. Degree in Information Security & Intelligence
***** Effective Fall 2012 *****
Wayne County Community College District
Student Checksheet

NAME: _____ ID#: _____ DATE _____ ADVISOR: _____

Major Core Requirements (60 credits): WCCCD College equivalent courses are identified in third column. FSU classes are in bold. Highlighted courses are available online.

Required Courses	Course Title– FSU Prerequisites Shown in Parentheses ()	WCCCD Equivalent Courses	FSU S. H.	Planned	Completed	Grade
ACCT 201	Principles of Accounting (MATH 110 w/C- or better or 19 on ACT or 460 on SAT or one of the following MATH courses 115 to 120, 126, 130, 132, 135)	ACT 201	3			
MGMT 301	Applied Management	MGT 205	3			
MKTG 321	Principles of Marketing (sophomore status or instructor permit)	MKT 200	3			
MGMT 350	Tools for Decision Making	FSU class	3			
STQM 260	Introduction to Statistics (MATH 115, 116 or 117 or 24 ACT or 560 SAT)	BUS 231 or MAT 131	3			
STQM 270	Introduction to Data Mining (STQM 260)	FSU class	3			
STQM 360	Risk Analysis and Strategy (STQM 260)	FSU class	3			
ISYS 200	Database Design & Implementation (ISYS 105 or demonstrated competency)	CIS 285	3			
PROJ 320	Project Management	FSU class	3			
HSCJ 202	Principles of Information Security	FSU class				
HSCJ 310	Digital Forensics and Analysis (HSCJ 202)	FSU class	3			
HSCJ 317	Fraud Examination	FSU class	3			
ISIN 200	All Things Digital	FSU class	3			
ISIN 300	Visual Analysis and Investigations	FSU class	3			
ISIN 301	Data Intelligence Competitive Theory (ISIN 300, ISYS 200)	FSU class	3			
ISIN312	Applications of Information Security (HSCJ 202)	FSU class	3			
ISIN 390	Special Topics in ISIN	FSU class	3			
ISIN 429	Legal & Ethical Issues in Information Security	FSU class	3			
ISIN 491	Internship	FSU class	3			
ISIN 499	Capstone Experience (Senior Standing)	FSU class	3			
Total						
Major Core Credits Required: 60 credits						
Directed Electives: 7-8 Credits Required (to total 120 credits for the BS Degree)						
Note: Discuss with Advisor - 300-400 level classes may be needed here to fulfill the 40 credit 300-400 level requirements in the degree						
		FSU or WCCCD	3			
		FSU or WCCCD	3			
		FSU or WCCCD	1-2			

Concentration or an approved minor (12 Credits Required)						
Digital Forensics						
HSCJ 315	Advanced Digital Forensics (HSCJ 310)	FSU Class	3			
ISYS 216	Intro to Java Programming (ISYS 110)	CIS 259 or CIS 207	3			
ISYS 371	Advanced Database Design & Implementation (ISYS 200 & ISYS 216)	CIS 246	3			
ISYS 325	Networking Essentials (ISYS 105 or demonstrated competency)	CIS 287	3			
Network Security						
ISYS 277	Linux Network Administration	CIS 240	3			
ISYS 325	Networking Essentials (ISYS 105 or demonstrated competency)	CIS 287	3			
	Elective		3			
	Elective		3			
National Security						
ISIN 350	Organizational Planning and Security Measures	Ferris class	3			
ISIN 351	Global Security and Policy	Ferris class	3			
ISIN 352	Role of Intelligence in National Security	Ferris class	3			
	Approved Elective		3			
Project Management (Online)						
PROJ 350	Project Schedule, Cost and Risk Management	Ferris class	3			
PROJ 351	Project Communication, Team Building and Conflict Management	Ferris class	3			
PROJ 420	Managing the Procurement Process and Preparing for the PMP	Ferris class	3			
MGMT 370	Quality-Operations Management	Ferris class	3			
Foreign Language						
	Foreign Language 1		3			
	Foreign Language 2		3			
	Foreign Language 3		3			
	Foreign Language 4		3			

General Education Requirements (40-41 Credits):

EARNED MACRAO STAMP: YES NO

Required Courses	Course Title FSU Prerequisites Shown in Parentheses ()	WCCCD Equivalent Courses	FSU S.H.	Planned	Completed	Grade
Communication Competence—12 Credits Required						
COMM ELEC	COMM 105, Interpersonal Communication or COMM 121, Fundamentals of Public Speaking	SPH 100 or SPH 101	3			
ENGL 150	English 1 (ENGL 074 w/C- or better or 14 > ACT or 370 > SAT)	ENG 110	3			
ENGL 211 or ENGL 250	Industrial and Career Writing (ENGL 150 w/C- or better) English 2 (ENGL 150 w/C- or better)	ENG 270	3			
ENGL 311 or ENGL 321 or ENGL 325	Advanced Technical Writing (ENGL 250 or ENGL 211 w/C or better) Advanced Composition (ENGL 250 or ENGL 211 w/C or better) Advanced Business Writing (ENGL 250 or ENGL 211 w/C or better)	FSU Class	3			
Scientific Understanding – 7 to 8 Credits Required						
This requirement can be met with science courses in the following areas: Astronomy, Biology, Chemistry, Geology, Physical Science, Physics, or FSU's GEOG 111 or GEOG 121						
	Scientific Understanding Elective with Lab		4			
	Scientific Understanding Elective (Lab or Non-Lab)		3 or 4			
Quantitative Skills – This requirement can be completed by one of the following options: (1) pass Math 115 or higher, (2) pass course proficiency exam in Math 115 or higher, (3) pass the College Algebra CLEP exam, or (4) an ACT math subtest score of 24 or higher.						
MATH 115	Intermediate Algebra (ACT of 19-21 or SAT of 350- 450)	MAT 113	3			
Cultural Enrichment – 9 Credits Required						
Credits can be earned in one or more subject areas; however, one three-credit course must be at the 200 level or higher. Select from the following subject areas: Art, Art History, any foreign language (German, Spanish or French at WCCCD), History, Humanities, Literature, Music, Philosophy (but not Logic), or Theatre.						
	Cultural Enrichment Elective	WCCCD or MACROA	3			
	Cultural Enrichment Elective	WCCCD or MACROA	3			
	Cultural Enrichment Elective (200 level or above)	WCCCD or MACROA	3			
Social Awareness – 9 Credits Required						
Subject areas include: Anthropology, Economics, Geography (but not Physical Geography; this course is considered a science elective), Political Science, Psychology or Sociology. Criteria: (1) One three-credit course must be 200-level or higher. (2) Must have two subject areas.						
	Social Awareness Elective	WCCCD or MACROA	3			
	Social Awareness Elective	WCCCD or MACROA	3			
	Social Awareness Elective (200 level or above)	WCCCD or MACROA	3			
40-41 General Education Hours Required						

Advising Notes:

Global consciousness requirement satisfied by: _____

Race/Ethnicity/Gender requirement satisfied by: _____

Admission Requirements:

1. High school students must have a 3.0 cumulative GPA (on a 4.00 scale) and an ACT composite score of 22. College transfer students must have a 2.70 cumulative GPA to be admitted to this program.
2. Apply online at www.ferris.edu/offcampus and submit official high school or college transcripts and ACT scores to Ferris State University, Office of admissions and records, 1201 Campus Drive CSS201, Big Rapids, MI. 49307-2288
3. Admission to WCCCD College is also essential since many courses in the degree are completed through WCCCD as a dual enrolled student.
4. Financial aid is available when dually enrolled in classes at Ferris State University and WCCCD College. All financial aid will only originate with FSU to cover costs at both institutions. For more information regarding the financial aid process contact the main campus Financial Aid Office

Updated: February, 2011

Effective: Fall 2011 Semester

at 231-591-2110. For general financial aid questions you can also go to finaid@ferris.edu or for community college consortium questions go to cnsrtfinaid@ferris.edu.

Graduation Requirements:

1. A minimum of 120 semester credits must be completed for graduation – 40 of which must be 300 level or higher.
2. A 2.0 cumulative GPA is required in the major, concentration and overall for completion of the ISI degree.
3. At least 30 FSU semester credits must be completed to fulfill FSU residency requirements.
4. Students must meet the University General Education Requirements (*Refer to WCCCD guidance regarding meeting the Ferris General Education requirements and /or WCCCD MACRAO requirements*).

Ferris ISI Core Course Descriptions (3 credit classes)

HSCJ 202-Principles of Information Security

Students explore the concepts of information security from both historical and emerging perspectives. Topics include the capabilities and threats of technology to information security, computer crime, homeland security, as well as legal, ethical and professional issues. The history, nature, and extent of computer crime and the roles and responsibilities of the legal system will also be investigated.

HSCJ 310-Digital Forensics and Analysis

Students learn the fundamentals of digital evidence collection and analysis. Emphasis is on both the collection of digital evidence and on common analysis tasks. Students will utilize various digital forensic tools and techniques for collection and analysis of digital evidence.

HSCJ 315-Advanced Digital Forensics

Students explore advanced digital forensic techniques and develop skills to deal with situations requiring a sophisticated response. Emerging and next generation computer technologies and threats, as well as proactive security measures and threat prevention will also be investigated. Students will utilize several digital forensic tools and techniques for collection, analysis, and incident processing.

HSCJ 317-Fraud Examination

Students will examine the fundamental reasons of why people commit fraud. Participants will investigate and explore how opportunity, pressures and rationalization are linked together to foster an atmosphere that can allow fraud to occur. Additionally, students will learn basic examination techniques for discovering fraud and more importantly, how to deter fraud from taking place.

ISIN 200-All Things Digital

Students investigate various digital devices including computers, cameras, surveillance equipment, and small devices and how to utilize them to advance security objectives. Students also work with various forms of media to understand the capabilities of each. Communication methods and networking are also explored.

ISIN 300-Visual Analysis Investigations

Introduction to transforming information into a visual format for analysis, interpretation and reporting. Students learn to deal with investigative issues involved to gather information, digital implications and strategies for effectively dealing with data from multiple sources. Analysis of digital data such as phone and financial records, surveillance information and visual media.

ISIN 301-Data-intelligence Comp Theory

Students examine the scientific process as it applies to hypothesis development. Investigation includes the analysis of various approaches to explaining events and developing competing hypothesis. The role of data and information in the development and support of intelligence in organization, national and international realms is also studied.

ISIN 312-Applications of Information Security

Students apply the tools and concepts of information security to mitigate and respond to risks. The theory and operation of information security tools and techniques are discussed, and students design and test their application in a variety of scenarios. Topics include software-, hardware-, host-, and network-based solutions.

ISIN 390-Special Topics in ISIN

This course covers various topics taught by diverse faculty.

ISIN 429-Legal-Ethical Issues Information Security

This course is intended to investigate the legal and ethical issues in Information Security. Ethical practices, privacy, copyright and licensing issues are research. Issues dealing with proprietary and personal information, as well as electronic technologies will be studied. An understanding of current and future impact on information systems and management strategies will be explored.

ISIN 499-Capstone Experience

This course provides students with an opportunity to demonstrate the skills and knowledge they have obtained in their program through project and/or portfolio methodologies and how they would be utilized in the workplace. Students will also investigate how information security is incorporated in their chosen path.

ISYS 371-Adv. Database Design and Implementation

Emphasis is placed on Entity-Relationships and Relational models, data definition languages, and manipulation languages. Structured Query Language (SQL) is used to develop database objects such as databases, logs, tables, indexes, views, constraints, defaults, roles, rules, stored procedures, and triggers. Database design is reviewed. Application development and modeling tools are discussed. Projects requiring the development of integrated databases are assigned.

PROJ 320-Project Management

An in-depth study of project management techniques currently employed for business and information systems projects. Topical areas will include project organization, planning and administration control and leadership. The need for accurate estimating, scheduling, communicating and reporting will be stressed through the use of several cases/projects. Senior Status

STQM 360-Risk Analysis and Strategy

Introduction to risk analysis and strategic approaches, principles, practices, tools, technology, and software. Risk analysis tools and approaches (e.g. planning, structured risk assessment, research and information discovery, probability and expectation, prioritization). Risk strategies, disposition, decision support, human resource development/management, and improvement/change strategies and tools. Application of risk analysis software. Applications and case studies to industry-specific events and projects (e.g. sport entertainment, security).

STQM 270-Introduction to Data Mining

Explore the relationship between data mining, data warehousing, and organizational needs. Explore basic data mining processes, methods and tools in varied areas of application such as business, manufacturing, healthcare, education, criminal justice, or government. Explore knowledge requirements across varied application areas as well as robust data mining processes and tools to serve varied needs. Case studies illustrate varied knowledge needs and data mining processes, methods, and tools. Introduces basic data mining software (e.g. WEKA, Excel based, or SPSS based).

Bachelor of Science INFORMATION SECURITY & INTELLIGENCE

Serving the Military – ISI Online (Effective Fall 2013)

As the only program of its kind in the country, Ferris Information Security & Intelligence (ISI) Program is at the forefront in its response to the need for skilled workers in Information Security/Data Analysis/Digital Investigation and Forensics. Developed with input from the U.S. Department of Homeland Security, the Pentagon, and investigative agencies; providing hands on utilization of state of the art technology, this program is uniquely positioned to satisfy the education credential necessary for students to be licensed as Professional Investigators in the State of Michigan, while our computer forensics coursework is accepted for meeting the education requirement to site for computer forensic examinations. In June 2011, Ferris State University formally received its designation as National Center of Academic Excellence in IA Education (CAE/IAE) by the NSA (National Security Agency), DOD (Department of Defense) and the DHS (Department of Homeland Security). Ferris successfully mapped its ISI (Information Security & Intelligence) and ISM (Information System Management) programs classes against all six NSA standards making it one of very few universities in the country to have achieved that level of mapping and the CAE/IAE designation.

General Admission Criteria

ISI Online is a Degree Completion Program that builds upon the 48 credit hour general education courses obtained at an educational institution of your choice. To be admitted to this program you must have a minimum 2.7 cumulative GPA in 48+ credits as a transfer student. As part of your application process, you will need to submit official transcripts from all colleges/universities you have attended. There is no cost to apply to Ferris which can be accessed via

Course Requirements

General Education Transferred Credits (FSU equivalencies are in parentheses)

General Education Requirements (satisfied by MACRAO Stamp and courses that meet transfer equivalencies at other academic institutions)

COMM 105 Interpersonal Communication or COMM 121 Oral Communication	3
ENG 150 Composition I	3
ENG 250 Composition II	3
Scientific Understanding w/Lab	4
Scientific Understanding without Lab	3
Cultural Enrichment Electives (See FSU Advisor)	9
Social Awareness Electives (See FSU Advisor)	9
MTH 115 Intermediate Algebra	3

Business Core Courses

STQM 260 Elementary Statistics	3
ACC 201 Principles of Accounting 1	4
MMGT 301 Applied Management	3
MKTG 321 Principles of Marketing	3
ISYS 200 Database Design	3

Ferris State University

General Education Courses

ENG 311 or 321 or 325 Advanced Writing	3
--	---

Business Core Courses

MGMT 350 Tools for Decision Making	3
------------------------------------	---

Information Security & Intelligence Major Core

STQM 270 Introduction to Data Mining	3
STQM 360 Risk Analysis and Strategy	3
ISIN 200 All Things Digital	3
HSCJ 202 Principles of Information Security	3
HSCJ 310 Digital Forensics and Incident Response	3
PROJ 320 Project Management Fundamentals	3
ISCI 317 Fraud Examination	3
ISIN 429 Legal and Ethical Issues in Security	3
ISIN 300 Visual Analysis	3

ISIN 301 Data Intelligence Competitive Theory	3
ISIN 312 Applications of Information Security	3
ISIN 390 Special Topics in Information Security	3
ISIN 491 Internship	3
ISIN 499 Capstone (Senior Standing)	3
Directed Electives	4-7

ISI Concentrations

Digital Forensics

HSCJ 315 Advanced Digital Forensics (CST 183)	3
ISYS 216 Java (CST 183)	3
ISYS 325 Networking Essentials (CST 161)	3
ISYS 371 Advanced Database (CST 159 & 259)	3

Project Management

PROJ 350 Project Scheduling	3
ISYS 351 Project Communication	3
PROJ 420 Project Procurement & PMP Prep	3
MGMT 370 Quality Operations Management	3

National Security

ISIN 350 Organizational Planning and Security Measures	3
ISIN 351 Global Security and Policy	3
ISIN 352 The Role of Intelligence	3
Approved Elective	3

Total Gen Ed Credits	40
Total Business Core Credits	16
Total Ferris Business Core Credits	6
Total ISI Core Credits	42
Total Concentration Credits	12
Directed Electives Credits	4-7
TOTAL CREDITS	120

For more information, visit us online.

http://isl.ferris.edu/ISI_Home.html

Dr. Barbara Ciaramitro (Dr. C) ciaramb@ferris.edu or 313 207-6127

Appendix E: TracDat Reports

Assessment Impact by Unit Objectives

Ferris State University

Program - Information Security and Intelligence (B.S.)

Program - Information Security and Intelligence (B.S.)

Mission Statement: The mission of the Information, Security and Intelligence degree is to prepare students for work in the digital age. Our goal is to provide the best possible training in the acquisition, manipulation, reconstruction, analysis and presentation of digital information.

Advisory Board/Committee Once per year

Meetings:

Next FSU Academic 2012-2013

Program Review:

Accreditation Body: Committee on National Security Systems (National Security Agency & Dept of Homeland Security)

Academic Year of Next 2015-2016

Accreditation Review:

College: COB

Outcome: ISI Program Outcomes - End of Program : End of program outcomes for Information Security & Intelligence

Evaluation of ISI program outcomes

Outcome Type: Learning

Start Date: 08/30/2010

Outcome Status: Active

Means of Assessment

Assessment Method	Criterion for Success	Assessment Schedule	Active
Students will submit an e-portfolio as part of the requirements for their capstone project. Portfolio will include at least 10 assignments/projects from various classes in the student's program. Assessment Method Category: Portfolio/E-Portfolio	Successfully demonstrate that they have understanding and competence in portfolio areas.	Conclusion of capstone course.	Yes
Capstone project must be written and presented. Project must be in a topic area that is consistent with ISI curriculum and student area of study. Assessment Method Category: Written Product (essay, research paper, journal, newsletter, etc.)	Successfully demonstrate understanding and fluency in selected topic area.	conclusion of capstone course.	Yes
Graduate survey - currently conducted via Zoomerang. Assessment Method Category: Survey - Graduate (Current Year)	Results received and analyzed.	Conclusion of capstone course.	Yes

Results

Result	Action	Follow-Up	Action
Survey - Graduate (Current Year) - 04/26/2012 - End of program survey - cumulative Classification: Criterion Met Related Documents: ISI 2010 Student-FawData.csv			2 - Pending Action
Survey - Graduate (Current Year) - 04/26/2012 - Survey results attached. Strong feedback on writing too many papers. Desire for stronger computer skills. Classification: Criterion Met			2 - Pending Action

Results			
Result	Action	Follow-Up	Action
Written Product (essay, research paper, journal, newsletter, etc.) - 12/22/2010 - The written portion of the capstone projects were well done and demonstrated strong student understanding of the topic area. The presentations were either via Adobe Connect Pro (teleconference), submitted PowerPoint, or poster sessions at graduation reception. Presentations were the weak part. It is clear that students focus on the written portion and the presentations are an after thought. Would like to see the presentations strengthened and more emphasis will be placed on this in coming semesters. Classification: Criterion Met			3 - Action Completed
Portfolio/E-Portfolio - 12/22/2010 - The portfolios submitted by the capstone students exceeded expectations. Portfolios indicate a strong understanding of end of program outcomes. Classification: Criterion Met			1 - No Action Required
Survey - Graduate (Current Year) - 12/22/2010 - Results indicate that GIS, Risk, and Data Mining are areas where curriculum/delivery can be improved. Student feedback also indicates that they would like more time in the forensics courses. Overall students give ISI program strong satisfaction scores. This survey is the baseline. Classification: Criterion Met Related Documents: ISI 2010 fall grad results	12/22/2010 - Shared survey with faculty and dept. heads.		2 - Pending Action

Outcome: National Security Agency Center of Excellence

Obtain and Maintain designation as NSA Center of Excellence.

Outcome Type: Other

Start Date: 08/27/2010

Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
NSA Accreditation process Assessment Method Category: Z - Other - specify	Pass/Fail	August - November, 2010	Yes

Results			
Result	Action	Follow-Up	Action
Z - Other - specify - 12/22/2010 - Received notification November 2010 that the ISI program has received Center of Excellence in all 6 NSA criteria areas. This makes Ferris the 6th university in the nation to achieve this. Classification:			3 - Action Completed

Results			
Result	Action	Follow-Up	Action
Criterion Met			
12/17/2010 - Survey shows graduates feedback on curriculum and Ferris processes. Survey confirms curriculum changes that were entered into the curricular process 11/2010. Classification: Criterion Met			3 - Action Completed

Outcome: Core Outcome #1 has been folded into other outcomes - delete. GG 8/25/10

Identify cultural and religious practices and explain how they may impact how a person or organization may operate.

Outcome Type: Learning

Outcome Status: Active

Related Courses

- HSCJ 202 - Principles of Info Security
- ISYS 411 - Project Management

Results			
Result	Action	Follow-Up	Action
06/25/2009 - Based on advisory board input and employer input, the program was changed from requiring RELG 326 Western Religions and a year of foreign language to recommended. Some community colleges (including Northwestern) do not count the first year of foreign language toward a degree, and this would add an additional year of foreign language study to a student's program.	05/05/2009 - modify curriculum		3 - Action Completed
Classification: Criterion Met			

Outcome: Core Outcome #3

Work as a member of an information security and/or intelligence team and effectively integrate theories and practice in an ISI environment.

Outcome Type: Learning

Outcome Status: Active

Related Courses

- HSCJ 202 - Principles of Info Security

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Outcome: Core Outcome #4

Theorize ways digital devices could be used for security and criminal activity and collect and process digital information in support of an investigation or hypothesis

Outcome Type: Learning

Outcome Status: Active

Related Courses

- HSCJ 210 - Digital Forensics

- HSCJ 317 - Fraud Examination
- ISIN 200 - All Things Digital

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Outcome: Core Outcome #5

Develop skills for evaluating organizational structure, environment, and planning strategies for security risk and analyze the effectiveness of a security plan against the methods used by organized crime, gangs and terrorist organizations.

Outcome Type: Learning

Outcome Status: Active

Related Courses

- HSCJ 202 - Principles of Info Security
- HSCJ 317 - Fraud Examination

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Outcome: Core Outcome #6

Design, construct and maintain databases in a format consistent with data mining. Analyze these structures in a temporal manner and present findings using a variety of methods including visual analysis tools and techniques.

Outcome Type: Learning

Outcome Status: Active

Related Courses

- ISYS 200 - Database Design-Implementation

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Outcome: Core Outcome #7

Recognize the potential for multiple explanations for events and information and be able to analyze and describe the accuracy of the information.

Outcome Type: Learning

Outcome Status: Active

Related Courses

- HSCJ 210 - Digital Forensics
- HSCJ 317 - Fraud Examination
- ISIN 301 - Data-Intelligence Comp Theory

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Outcome: Core Outcome #8

Utilize digital forensic tools and encryption technology to reconstruct information and recover lost or deleted files in a variety of digital platforms and settings using appropriate methodologies.

Outcome Type: Learning

Outcome Status: Active

Related Courses

- HSCJ 202 - Principles of Info Security
- HSCJ 210 - Digital Forensics

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Outcome: Core Outcome #9

Set up computer networks and peripheral devices, install and maintain software; demonstrate how to handle, transport, utilize and safeguard digital devices and information.

Outcome Type: Learning

Outcome Status: Active

Related Courses

- HSCJ 202 - Principles of Info Security
- HSCJ 210 - Digital Forensics
- ISIN 200 - All Things Digital

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Outcome: Core Outcome #10

Demonstrate knowledge of concepts and methodologies in information security and the Information Security Lifecycle (Protection) including information security administration, Security+ and CISSP.

Outcome Type: Learning

Outcome Status: Active

Related Courses

- HSCJ 202 - Principles of Info Security

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Outcome: Digital Forensics Concentration

Demonstrate knowledge of concepts and methodologies of incidence response, cyber forensics (acquisition, preservation, analysis, and presentation of evidence) and the information security lifecycle including cyber laws, cyber crimes, incidence response, pre-incident preparation, detection, notification, initial response, strategic decisions, response, recovery, and reporting

Outcome Type: Learning

Outcome Status: Active

Related Courses

- HSCJ 202 - Principles of Info Security
- HSCJ 210 - Digital Forensics
- HSCJ 317 - Fraud Examination

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Outcome: GIS and Data Mining Concentration

Demonstrate knowledge of business intelligence and GIS data and the evaluation of analytical data used in strategic decision making including knowledge discovery, tracking, managing and understanding organized data. Students will construct GIS and data mining environments using appropriate tools, techniques, decision support systems, and emerging trends.

Outcome Type: Learning

Outcome Status: Active

Related Courses

- ISYS 200 - Database Design-Implementation
- STQM 260 - Introduction to Statistics

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Outcome: National Security Concentration - i process of being removed from program. GG 8/25/10

Demonstrate an understanding of the components and challenges, and application of security initiatives. Components include project definition, team structure and communication, and project monitoring and evaluation.

Outcome Type: Learning

Outcome Status: Active

Related Courses

- HSCJ 317 - Fraud Examination
- ISYS 411 - Project Management

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Outcome: ISI Program Outcomes - End of Program : End of program outcomes for Information Security & Intelligence program (Copy)

Evaluation of ISI program outcomes

Outcome Type: Learning

Start Date: 08/30/2010

Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Students will submit an e-portfolio as part of the requirements for their capstone project. Portfolio will include at least 10 assignments/projects from various classes in the student's program. Assessment Method Category: Portfolio/E-Portfolio	Successfully demonstrate that they have understanding and competence in portfolio areas.	Conclusion of capstone course.	Yes
Capstone project must be written and presented. Project must be in a topic area that is consistent with ISI curriculum and student area of study. Assessment Method Category: Written Product (essay, research paper, journal, newsletter, etc.)	Successfully demonstrate understanding and fluency in selected topic area.	conclusion of capstone course.	Yes
Graduate survey - currently conducted via Zoomerang. Assessment Method Category: Survey - Graduate (Current Year)	Results received and analyzed.	Conclusion of capstone course.	Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

**Unit Assessment Report - Four Column

Ferris State University

Program - Information Security and Intelligence (B.S.)

Mission Statement: The mission of the Information, Security and Intelligence degree is to prepare students for work in the digital age. Our goal is to provide the best possible training in the acquisition, manipulation, reconstruction, analysis and presentation of digital information.

Advisory Board/Committee Meetings: Once per year

Next FSU Academic Program Review: 2012-2013

Accreditation Body: Committee on National Security Systems (National Security Agency & Dept of Homeland Security)

Academic Year of Next Accreditation Review: 2015-2016

College: COB

Outcomes	Means of Assessment & Criteria for Success / Tasks	Results	Action & Follow-Up
Program - Information Security and Intelligence (B.S.) - ISI Program Outcomes - End of Program : End of program outcomes for Information Security & Intelligence program - Evaluation of ISI program outcomes Outcome Types: Learning Start Date: 08/30/2010 Outcome Status: Active	Assessment Method: Students will submit an e-portfolio as part of the requirements for their capstone project. Portfolio will include at least 10 assignments/projects from various classes in the student's program. Assessment Method Category: Portfolio/E-Portfolio Criterion for Success: Successfully demonstrate that they have understanding and competence in portfolio areas.	12/22/2010 - The portfolios submitted by the capstone students exceeded expectations. Portfolios indicate a strong understanding of end of program outcomes. Classification: Criterion Met Action: 1 - No Action Required	
	Assessment Method: Capstone project must be written and presented. Project must be in a topic area that is consistent with ISI curriculum and student area of study. Assessment Method Category: Written Product (essay, research paper, journal, newsletter, etc.) Criterion for Success: Successfully demonstrate understanding and fluency in selected topic area.	12/22/2010 - The written portion of the capstone projects were well done and demonstrated strong student understanding of the topic area. The presentations were either via Adobe Connect Pro (teleconference), submitted PowerPoint, or poster sessions at graduation reception. Presentations were the weak part. It is clear that students focus on the written portion and the presentations are an after thought. Would like to see the presentations strengthened and more emphasis will be placed on this in coming semesters. Classification:	

Outcomes	Means of Assessment & Criteria for Success / Tasks	Results	Action & Follow-Up
<p>Intelligence (B.S.) - National Security Agency Center of Excellence - Obtain and Maintain designation as NSA Center of Excellence.</p> <p>Outcome Types: Other</p> <p>Start Date: 08/27/2010</p> <p>Outcome Status: Active</p>	<p>Assessment Method: NSA Accreditation process</p> <p>Assessment Method Category: Z - Other - specify</p> <p>Criterion for Success: Pass/Fail</p>	<p>12/22/2010 - Received notification November 2010 that the ISI program has received Center of Excellence in all 6 NSA criteria areas. This makes Ferris the 6th university in the nation to achieve this.</p> <p>Classification: Criterion Met</p> <p>Action: 3 - Action Completed</p> <hr/> <p>12/17/2010 - Survey shows graduates feedback on curriculum and Ferris processes. Survey confirms curriculum changes that were entered into the curricular process 11/2010.</p> <p>Classification: Criterion Met</p> <p>Action: 3 - Action Completed</p> <p>Change Assessment Strategy: Yes</p>	
<p>Program - Information Security and Intelligence (B.S.) - Core Outcome #1 has been folded into other outcomes - delete.</p> <p>GG 8/25/10 - Identify cultural and religious practices and explain how they may impact how a person or organization may operate.</p> <p>Outcome Types: Learning</p> <p>Outcome Status: Active</p>		<p>06/25/2009 - Based on advisory board input and employer input, the program was changed from requiring RELG 326 Western Religions and a year of foreign language to recommended. Some community colleges (including Northwestern) do not count the first year of foreign language toward a degree, and this would add an additional year of foreign language study to a student's program.</p> <p>Classification: Criterion Met</p> <p>Action: 3 - Action Completed</p>	<p>05/05/2009 - modify curriculum</p> <hr/>
<p>Program - Information Security and Intelligence (B.S.) - Core Outcome #3 - Work as a member of an information security and/or intelligence team and effectively integrate theories and practice</p>			

Outcomes	Means of Assessment & Criteria for Success / Tasks	Results	Action & Follow-Up
		<p>Criterion Met Action: 3 - Action Completed Change Assessment Strategy: Yes</p>	
	<p>Assessment Method: Graduate survey - currently conducted via Zoomerang. Assessment Method Category: Survey - Graduate (Current Year) Criterion for Success: Results received and analyzed.</p>	<p>04/26/2012 - End of program survey - cumulative Classification: Criterion Met Action: 2 - Pending Action Related Documents: ISI 2010 Student-RawData.csv</p>	
		<p>04/26/2012 - Survey results attached. Strong feedback on writing too many papers. Desire for stronger computer skills. Classification: Criterion Met Action: 2 - Pending Action</p>	
		<p>12/22/2010 - Results indicate that GIS, Risk, and Data Mining are areas where curriculum/delivery can be improved. Student feedback also indicates that they would like more time in the forensics courses. Overall students give ISI program strong satisfaction scores. This survey is the baseline. Classification: Criterion Met Action: 2 - Pending Action Change Assessment Strategy: Yes Curriculum Change: Does Not Require UCC Approval Related Documents: ISI 2010 fall grad results</p>	<p>12/22/2010 - Shared survey with faculty and dept. heads.</p> <hr/>

Program - Information Security and

Outcomes	Means of Assessment & Criteria for Success / Tasks	Results	Action & Follow-Up
<p>in an ISI environment.</p> <p>Outcome Types: Learning</p> <p>Outcome Status: Active</p>			
<p>Program - Information Security and Intelligence (B.S.) - Core Outcome #4 - Theorize ways digital devices could be used for security and criminal activity and collect and process digital information in support of an investigation or hypothesis</p> <p>Outcome Types: Learning</p> <p>Outcome Status: Active</p>			
<p>Program - Information Security and Intelligence (B.S.) - Core Outcome #5 - Develop skills for evaluating organizational structure, environment, and planning strategies for security risk and analyze the effectiveness of a security plan against the methods used by organized crime, gangs and terrorist organizations.</p> <p>Outcome Types: Learning</p> <p>Outcome Status: Active</p>			
<p>Program - Information Security and Intelligence (B.S.) - Core Outcome #6 - Design, construct and maintain databases in a format consistent with data mining. Analyze these structures in a temporal manner and present findings using a variety of methods including visual analysis tools and techniques.</p> <p>Outcome Types: Learning</p>			

Outcomes	Means of Assessment & Criteria for Success / Tasks	Results	Action & Follow-Up
<p>Outcome Status: Active</p> <p>Program - Information Security and Intelligence (B.S.) - Core Outcome #7 - Recognize the potential for multiple explanations for events and information and be able to analyze and describe the accuracy of the information.</p> <p>Outcome Types: Learning</p> <p>Outcome Status: Active</p>			
<p>Program - Information Security and Intelligence (B.S.) - Core Outcome #8 - Utilize digital forensic tools and encryption technology to reconstruct information and recover lost or deleted files in a variety of digital platforms and settings using appropriate methodologies.</p> <p>Outcome Types: Learning</p> <p>Outcome Status: Active</p>			
<p>Program - Information Security and Intelligence (B.S.) - Core Outcome #9 - Set up computer networks and peripheral devices, install and maintain software; demonstrate how to handle, transport, utilize and safeguard digital devices and information.</p> <p>Outcome Types: Learning</p> <p>Outcome Status: Active</p>			
<p>Program - Information Security and Intelligence (B.S.) - Core Outcome #10 - Demonstrate knowledge of concepts and</p>			

Outcomes	Means of Assessment & Criteria for Success / Tasks	Results	Action & Follow-Up
<p>methodologies in information security and the Information Security Lifecycle (Protection) including information security administration, Security+ and CISSP.</p> <p>Outcome Types: Learning</p> <p>Outcome Status: Active</p>			
<p>Program - Information Security and Intelligence (B.S.) - Digital Forensics Concentration - Demonstrate knowledge of concepts and methodologies of incidence response, cyber forensics (acquisition, preservation, analysis, and presentation of evidence) and the information security lifecycle including cyber laws, cyber crimes, incidence response, pre-incident preparation, detection, notification, initial response, strategic decisions, response, recovery, and reporting</p> <p>Outcome Types: Learning</p> <p>Outcome Status: Active</p>			
<p>Program - Information Security and Intelligence (B.S.) - GIS and Data Mining Concentration - Demonstrate knowledge of business intelligence and GIS data and the evaluation of analytical data used in strategic decision making including knowledge discovery, tracking, managing and understanding organized data. Students will construct GIS and data mining environments using appropriate tools, techniques, decision support systems, and emerging trends.</p> <p>Outcome Types: Learning</p> <p>Outcome Status:</p>			

Outcomes	Means of Assessment & Criteria for Success / Tasks	Results	Action & Follow-Up
Active			
<p>Program - Information Security and Intelligence (B.S.) - National Security Concentration - i process of being removed from program. GG 8/25/10 - Demonstrate an understanding of the components and challenges, and application of security initiatives. Components include project definition, team structure and communication, and project monitoring and evaluation.</p> <p>Outcome Types: Learning</p> <p>Outcome Status: Active</p>			
<p>Program - Information Security and Intelligence (B.S.) - ISI Program Outcomes - End of Program : End of program outcomes for Information Security & Intelligence program (Copy) - Evaluation of ISI program outcomes</p> <p>Outcome Types: Learning</p> <p>Start Date: 08/30/2010</p> <p>Outcome Status: Active</p>	<p>Assessment Method: Students will submit an e-portfolio as part of the requirements for their capstone project. Portfolio will include at least 10 assignments/projects from various classes in the student's program.</p> <p>Assessment Method Category: Portfolio/E-Portfolio</p> <p>Criterion for Success: Successfully demonstrate that they have understanding and competence in portfolio areas.</p>		
	<p>Assessment Method: Capstone project must be written and presented. Project must be in a topic area that is consistent with ISI curriculum and student area of study.</p> <p>Assessment Method Category: Written Product (essay, research paper, journal, newsletter, etc.)</p> <p>Criterion for Success: Successfully demonstrate understanding and</p>		

Outcomes	Means of Assessment & Criteria for Success / Tasks	Results	Action & Follow-Up
	<p>fluency in selected topic area.</p> <p>Assessment Method: Graduate survey - currently conducted via Zoomerang.</p> <p>Assessment Method Category: Survey - Graduate (Current Year)</p> <p>Criterion for Success: Results received and analyzed.</p>		

Assessment Impact by Course Objectives

Ferris State University

Z - ISIN Courses

Z - ISIN Courses

Course Outcome: ISIN 200 - All Things Digital: Small Device Investigations (Created By Z - ISIN Courses)

Investigate various digital devices including computers, cameras, surveillance equipment, and small devices and how to utilize them to advance security objectives.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment

Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	Successful completion of test	every semester offered	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successful Completion of Assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful Completion		Yes

Results

Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 200 - All Things Digital: Media Forms (Created By Z - ISIN Courses)

Work with various forms of media to understand the capabilities of each. Find and discuss articles on media storage devices

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment

Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	Successful completion of test	every semester offered	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results

Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 200 - All Things Digital: Operating Systems (Created By Z - ISIN Courses)

Find and discuss information on operating system options.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - External - Post or Pre/Post	Successful Test Completion	every semester offered	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 200 - All Things Digital: Imaging (Created By Z - ISIN Courses)

Find and discuss information on image editing/viewing software. Find and discuss info on digital camera options & features. Find and discuss information on image format choices.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing	Successfully complete test	every semester offered	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 200 - All Things Digital: Forensic Software (Created By Z - ISIN Courses)

Find and discuss articles on digital forensic software.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	Successfully complete test	every semester offered	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 200 - All Things Digital: HTML & XML (Created By Z - ISIN Courses)

Find and discuss articles on HTML and XML.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	Successfully complete test	every semester offered	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 200 - All Things Digital: Encryption (Created By Z - ISIN Courses)

Find and discuss articles on encryption.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	Successfully complete test	every semester offered	Yes

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 220 - Visual Analysis-Investigations: Visual Analysis/Investigative Process (Created By Z - ISIN

Identify, describe and outline the visual analysis and investigative process.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	Successful test completion	by semester	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 220 - Visual Analysis-Investigations: Visual Analysis Environment (Created By Z - ISIN Courses)

Construct a visual analysis environment for data investigation.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	Successfully complete test	Every semester offered.	Yes
Team Role Play/Scenario Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion		Yes

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
Project/Model/Invention - 04/26/2012 - Students utilized i2 for Visual mapping and analysis of several scenarios including pattern recognition. Results indicated that about one-quarter of the students are stuck on the intricacies of the technology and don't see the big picture. This may be due to technical skills as it appears CJ students and those with weak technical background feel technical intimidation. Classification: Criterion Met			1 - No Action Required

Course Outcome: ISIN 220 - Visual Analysis-Investigations: Information Interpretation (Created By Z - ISIN Courses)

Demonstrate how to utilize a visual analysis environment for information interpretation.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	Successfully complete test	Every semester offered.	Yes
Role Play/Scenario Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 220 - Visual Analysis-Investigations: Temporal/Associative Characteristics of Information (Created By Z - ISIN Courses)

Comprehend and interpret temporal and associative characteristics of information.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	Successfully complete test	Every semester offered.	Yes
Role Play/Scenario Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
Project/Model/Invention - 04/26/2012 - Students submitted temporal analysis of Virginia Tech shooting. Visual analysis techniques utilized provided insight into actual issues surrounding the event. Classification: Criterion Met			1 - No Action Required

Course Outcome: ISIN 301 - Data-Intelligence Comp Theory: Scientific Process (Created By Z - ISIN Courses)

Demonstrate an understanding of the scientific process and hypothesis development.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	Successful completion of test	every semester offered	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 301 - Data-Intelligence Comp Theory: Hypothesis Development (Created By Z - ISIN Courses)

Construct and interpret information used in hypothesis development and evaluation.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	Successful testing	every semester offered	Yes
Assignment- Team Role Play/Scenario Study Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of assignment		Yes
Assignment - ACH Assessment Method Category: Project/Model/Invention	Successful completion of Assignment		Yes

Results			
Result	Action	Follow-Up	Action
Case Studies/Problem-based Assignments - 04/26/2012 - Evaluation of readings indicated that students learned that they had preconceptions that would bias study design and interpretation. Every student indicated this was an eye opening experience. Classification: Criterion Met			1 - No Action Required
Project/Model/Invention - 04/26/2012 - Students utilized ACH toolkit to evaluate competing hypothesis. Teams had to present their methods and findings. All teams completed assignment, though some had difficulty grasping correct phrasing of hypothesis and testing methods. Classification: Criterion Met			1 - No Action Required

Course Outcome: ISIN 301 - Data-Intelligence Comp Theory: Analyze Hypotheses (Created By Z - ISIN Courses)

Students will analyze hypotheses and apply various approaches to credit or discredit (e.g. falsification).

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	Successful testing	every semester offered	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results

Results			
Result	Action	Follow-Up	Action
Project/Model/Invention - 04/26/2012 - Use of ACH to evaluate competing hypothesis - students present anticipated as well as actual results. Approximately half the class found that they had preconceived bias that was borne out in the ACH model. Classification: Criterion Met			1 - No Action Required

Course Outcome: ISIN 301 - Data-Intelligence Comp Theory: Intelligence (Created By Z - ISIN Courses)

Students will distinguish between predictive and retroactive intelligence and proper application of information evaluation.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	Successful testing	every semester offered	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
Case Studies/Problem-based Assignments - 04/26/2012 - Students completed several selected readings that dealt with varying perspectives that would influence analysis, evaluation, and interpretation. Exercises generated desired result and student evaluation of achieving this outcome was constructively positive. Classification: Criterion Met			1 - No Action Required

Course Outcome: ISIN 330 - Org Crime-Gang-Terrorist Org: Concepts (Created By Z - ISIN Courses)

Understand conceptual framework for studying the problem of organized crime, gangs and terrorism.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing	successfully complete test	every semester offered	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 330 - Org Crime-Gang-Terrorist Org: Organized Crime (Created By Z - ISIN Courses)

Understand historical background on organized crime, gang and terrorist organizations. Identify and describe organized crime, gang and terrorist organizations and their culture.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing	successfully complete test	every semester offered	Yes
Assessment Method Category: Test - Internally Developed - Pre/Post or Post			
Assignment	Successful completion of assignment		Yes
Assessment Method Category: Case Studies/Problem-based Assignments			
Assignment	Successful completion of assignment		Yes
Assessment Method Category: Project/Model/Invention			

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 330 - Org Crime-Gang-Terrorist Org: Criminal Techniques (Created By Z - ISIN Courses)

Develop skills for evaluating the effectiveness of the techniques used by organized crime, gang and terrorist organizations.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing	successfully complete test	every semester offered	Yes
Assessment Method Category: Test - Internally Developed - Pre/Post or Post			

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 330 - Org Crime-Gang-Terrorist Org: Counter Methods (Created By Z - ISIN Courses)

Analyze the methods used to combat organized crime, gangs and terrorism.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	successfully complete test	every semester offered	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of Assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 330 - Org Crime-Gang-Terrorist Org: Impact Mitigation (Created By Z - ISIN Courses)

Theorize on ways to mitigate the impact of organized crime, gang and terrorist organizations.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	successfully complete test	every semester offered	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successfully complete assignment		Yes

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 350 - Org Planning-Security Measures: Evaluation Techniques (Created By Z - ISIN Courses)

Develop skills for evaluating organizational structure, environment, and planning strategies for risk.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	Successfully complete test	every semester offered	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 350 - Org Planning-Security Measures: Security Plan (Created By Z - ISIN Courses)

Identify and describe the characteristics of a security plan, implementation plan, and execution strategy.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	Successfully complete test	every semester offered	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successfully complete assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successfully complete assignment		Yes

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 350 - Org Planning-Security Measures: Countermeasures (Created By Z - ISIN Courses)

Analyze security and risk plans and develop countermeasure plans.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	Successfully perform test	every semester offered	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 350 - Org Planning-Security Measures: Organizational Plan Assessment (Created By Z - ISIN Courses)

Scrutinize and organization's planning and security measures, and develop improvement strategies.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	Successfully complete test	every semester offered	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successfully complete assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successfully complete assignment		Yes

Results			
Result	Action	Follow-Up	Action

No Results reported.

Course Outcome: ISIN 429 - Legal-Ethical Issues Infor Sec: Moral/Legal Issues (Created By Z - ISIN Courses)

Analyze the moral and legal dilemmas that arise in the areas of free speech, intellectual property, privacy, licensing, and security.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	successfully completing test	Each semester offered.	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 429 - Legal-Ethical Issues Infor Sec: Global IT Ethics (Created By Z - ISIN Courses)

Develop and understanding of the ever-increasing global nature of IT ethics and how ethical/unethical decisions impact the global community.

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	successfully completing test	Each semester offered.	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 429 - Legal-Ethical Issues Infor Sec: Generational Differences (Created By Z - ISIN Courses)

Gain a better understanding of various generational differences, which people possess, based on the historical events that occurred during their childhood, and how those differences shape individual values as a basis for personal decision-making.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	successfully completing test	Each semester offered.	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of Assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 429 - Legal-Ethical Issues Infor Sec: Ethics Application (Created By Z - ISIN Courses)

Investigate and provide practice in applying a code of ethics and professional conduct to actual or hypothetical case studies.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Objective testing Assessment Method Category: Test - Internally Developed - Pre/Post or Post	successfully completing test	Each semester offered.	Yes
Assignment Assessment Method Category: Case Studies/Problem-based Assignments	Successful completion of assignment		Yes
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 499 - Capstone Experience: Project (Created By Z - ISIN Courses)

Create and present a project and/or portfolio that demonstrate integration of the end of program outcomes.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Presentation Assessment Method Category: Presentation(Oral)	Successfully complete presentation	Every semester offered.	Yes

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Assignment Assessment Method Category: Project/Model/Invention	Successful completion of assignment		Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Course Outcome: ISIN 499 - Capstone Experience: Career Path (Created By Z - ISIN Courses)

Investigate how information security and intelligence is incorporated in the student's chosen career path.

Start Date: 07/01/2009

Course Outcome Status: Active

Means of Assessment			
Assessment Method	Criterion for Success	Assessment Schedule	Active
Project assessment. Assessment Method Category: Project/Model/Invention	Successfully complete project.	Every semester offered.	Yes

Results			
Result	Action	Follow-Up	Action
No Results reported.			

Program - Information Security and Intelligence (B.S.) - Curriculum Map

Legend: (A) - Program Assessment, (I) - Introduced, (M) - Mastery, (R) - Reinforced

Outcomes	ACCT 201	COM 1	COM 2	ENGL 150	ENGL 211	ENGL 250	ENGL 311	ENGL 321	ENGL 325	HIST 257	HSCJ 202	HSCJ 210	HSCJ 317	ISIN 200	ISIN 220	ISIN 301	ISIN 429	ISYS 200	ISYS 411	ISYS 491	ISYS 497	MAT 111	MAT 303	MAT 353	MKTG 326	STQM 2020	STQM 2626	STQM 3636	SURRE 325	
ISI Program Outcomes - End of Program : End of program outcomes for Information Security & Intelligence program																														
National Security Agency Center of Excellence																														
Core Outcome #1 has been folded into other outcomes - delete. GG 8/25/10											I																			
Core Outcome #3											I																			
Core Outcome #4												A, I, R	R	I																
Core Outcome #5											R		R																	

Outcomes	ACCT 201	COMM	COMM	ENGL 150	ENGL 211	ENGL 250	ENGL 311	ENGL 321	ENGL 325	ENGL 325	HI 257	HS 202	HS 210	HS 317	ISIN 200	ISIN 220	ISIN 301	ISIN 429	ISYS 201	ISYS 411	ISYS 491	ISYS 497	MATH 111	MATH 303	MATH 353	MATH 323	RELG 326	STQM 202	STQM 262	STQM 363	SURE 325	
es for Information Security & Intelligence program (Copy)																																

Appendix F: ISI Program SWOT Analysis

Information Security & Intelligence SWOT Analysis and Program Goals

Based on the SWOT analysis on the following page, below is the list of ISI Program goals for the next academic year in order of priority.

- Expansion of ISI program to other locations
- Increase enrollment by 20% at each program location
- Work with new International Education Center to develop strong global partnerships with other universities around the world that results in faculty and student exchanges.
- Increase international enrollment in program.
- Work with New Incubator initiative to develop innovative new programs and opportunities.
- Develop marketing materials and plan marketing events to inform and promote the ISI program throughout Michigan.
- Develop Special Topic courses, seminars and conferences on topics identified by our Advisory Board including Business Intelligence, Mobile and Cloud Computing, Database and Database Security, Secure Application Development, Privacy, Risk, Compliance and Governance; and expand focus to encompass corporate security
- Work with new Grant Office to pursue grants through NSA and other funding sources
- Build strong student organization (ISIA)
- Achieve Quality Matters certification for online and hybrid courses
- Build strong diverse adjunct base to support expansion of program
- Partner with various organizations such as ISSA, Automation Alley, ISACS and with communities to professional networking and service learning opportunities for students

SWOT Analysis Template

Program: ISI (Information Security and Intelligence)

Date: August 23, 2011

Revised: November 16, 2011

Strengths	Weaknesses
<ul style="list-style-type: none">• Designated as NSA/DoD/DHS Center of Academic Excellence in Information Assurance• Mapped against all 6 of the NSA CNSS standards• Provides students with access to unique scholarship, internship and job opportunities• Strong interpersonal relationships with students through academic advising• Unique and highly rated undergraduate program offering in Michigan• Community colleges want partnerships• Successfully obtained grant for over \$300,000• Utilizes best in class forensic and analysis software• Established global educational partnership with Netherlands• Highly qualified faculty with advanced degrees and professional certifications• Mix of hybrid and online courses• Established dual enrollment program with students in Newago County.• Provides summer camp experiences for interested students	<ul style="list-style-type: none">• Need to increase global credibility through language training and relationships with other countries• No current program concentration offering in National Cyber Security, Global Cyber Security, Networking, or Secure Software Development• Weak student organization (ISIA)• Constant resource constraints in offering classes at all locations as often as desired.• Need to establish more campus partnerships with International Education Center and other departments and organizations• Limited community involvement• Limited service opportunities for students• Extensive travel for faculty
Opportunities	Threats
<ul style="list-style-type: none">• Expand program to other locations in Michigan aligning with Community Colleges• Develop an online version of the ISI program to serve the military• Opportunity to pursue grants through NSA and other funding sources due to CAE/IAE designation• Increase international enrollment in program.• Continue to develop innovative new programs and opportunities• Develop strong marketing initiatives to spread word about the ISI program and its CAE designation• Develop a strong student organization (ISIA) to increase student involvement• Develop online and hybrid programs that achieve Quality Matters designation• Supplement full time faculty with qualified and diverse adjunct base• Develop key partnerships with outside	<ul style="list-style-type: none">• Competition from Cyber Security online programs• Competition for qualified and diverse adjunct faculty• Faculty keeping abreast of current security issues and technology which is constantly evolving• Too few people doing too much• Extensive prep time for courses• Funding is a challenge to develop new programs, establish partnerships, and keep faculty up-to-date in current certifications and achievement of new certifications.

Appendix G: NSA Course Mapping



Information Security & Intelligence

Academic Program Review

*Attachment G – NSA Course
Mapping*

FERRIS STATE UNIVERSITY

2012

Barbara L Ciaramitaro, PhD
APR Committee Chair

APR Members
Douglas Blakemore, PhD
Greg Gogolin, PhD
Gerald Emerick, M.A.
Keith Jewett, M.S.

Appendix G: NSA Course Mapping

NSA Course Mapping Table of Contents

Description	Page
A. Organization Information	63
B. CNSS Standard NTSTISSI 4011	64
a. Course Mapping Details	65
b. Standard Specifications	66
C. CNSS Standard NTSTISSI 4012	67
a. Course Mapping Details	68
b. Standard Specifications	69
D. CNSS Standard NTSTISSI 4013	70
a. Course Mapping Details	71
b. Standard Specifications	72
E. CNSS Standard NTSTISSI 4014	73
a. Course Mapping Details	74
b. Standard Specifications	75
F. CNSS Standard NTSTISSI 4015	76
a. Course Mapping Details	77
b. Standard Specifications	78
G. CNSS Standard NTSTISSI 4016	79
a. Course Mapping Details	80
b. Standard Specifications	81
H. National Policy on Certification and Accreditation	82

A. Organization Information

Delete Print Edit Enter New Course Next Item Previous Item



Information Assurance Courseware Evaluation Program Course Information for Ferris State University

This Course Is Currently Being Taught:

Yes

Course Designator/Course Number:

HSCJ 202

Course Title:

Principles of Info Security

HTTP Link:

<http://catalog.ferris.edu/courses/HSCJ202/>

Course Length:

This 3 hour course consists of 45 hours of instruction over 7.5 weeks.

Course Description:




Students explore the concepts of information security from both historical and emerging perspectives. Topics include the capabilities and threats of technology to information security, computer crime, homeland security, as well as legal, ethical and professional issues. The history, nature, and extent of computer crime and the roles and responsibilities of the legal system will also be investigated.

Course Learning Objective:

1. Identify and describe Information Security concepts.
2. Identify and describe capabilities of technology as it relates to Information Security.
3. Identify and describe the threats to Information Security.
4. Investigate, assess, and summarize the various roles and responsibilities of government, law enforcement agencies, and the intelligence community in response, prevention and control of computer crime.
5. Examine the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)

Major Topics:

1. Information Security and Concepts
 - 1.1 Definition of information security
 - 1.2 Key events and precedents
 - 1.3 Professional standards and agencies/organizations
 - 1.4 Definitional importance and dilemmas - What is computer/cybercrime?
 - 1.5 Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)

 [Print](#)
 [Edit](#)
 [Request New Data Entry Person](#)



Information Assurance Courseware Evaluation Program Organization Information

The first step in the process of applying for IA Courseware Evaluation (IACE) is to provide information on your organization and to establish a point of contact for the process. You should have already contacted the CNSS IACE Program Office and received a password to allow you to electronically submit your application. Please provide the information requested below. While you may identify up to five data entry personnel, only the Point of Contact (POC) will be allowed to submit the organization's application. The POC will be provided passwords for the data entry personnel to use while entering the required information.

Institution Name: **Ferris State University**
Institution Internet URL: <http://www.ferris.edu/homepage.htm>
IACE Application URL: <https://app.cnss.gov/nietpcw369.nsf/>

Office / Program: College of Business/Accounting Finance
 Information Systems
Street: 119 S. State Street
City: Big Rapids
State: MI
Zip Code: 49307
Telephone: (231) 591-2434

Institution Point of Contact: **Barbara Ciaramitaro**
Title: Assistant Professor
Department: College of Business/Accounting Finance
 Information Systems
Street: 119 S. State Street
City: Biig Rapids
State: MI
Zip Code: 49307
Telephone: 231 591-3199
FAX:
Email: ciaramb@ferris.edu

Data Entry Personnel: If you would like to add a data entry person please use the "Request New Data Entry Person" button above.
 To remove a data entry person(s) please click on [this](#) and cut and paste the name(s) into the email.

Name: Robert Ewigleben

Name:
Name:
Name:

2. Capabilities of technology

- 2.1 Use/ability of technology
- 2.2 History and roles of technology in crime

3. Threats to Information Security

- 3.1 Victimization - types and new forms of victimization, disincentives to report, etc.
 - 3.2 Criminal tools and techniques
 - 3.3 Computer use by international organized crime and other "abusive" groups
 - 3.4 What is truly threatening (and for whom) versus what is popular/easy to enforce
- ## 4. Roles and responsibilities of government, law enforcement agencies, and the intelligence community
- 4.1 Federal agency roles and responsibilities
 - 4.2 Department of Homeland Security issues
 - 4.3 Homeland security and the war on terrorism

3. Threats

homeland security, as well as legal, ethical and professional issues. The history, nature, and extent and the roles and responsibilities of the legal system will also be investigated.

Method of Instruction:

Course is delivered in a mixed delivery format (in person and online instruction) consisting of:

1. Lectures
2. Individual and team hands-on exercises/demonstrations
3. Individual and team projects
4. Case study review and analysis
5. Individual online research and assignments







Evaluation Methods:

1. Objective testing (final exam)
2. Graded case study analysis and/or project assessment
3. Class and online participation/contributions assessment

Student Enrollment

Current Year: 50

Past Years: 46

 Delete	 Print	 Edit	 Enter New Course	 Next Item	 Previous Item
--	---	--	--	---	---



Information Assurance Courseware Evaluation Program Course Information for Ferris State University

This Course Is Currently Being Taught:

Yes

Course Designator/Course Number:

HSCJ 210

Course Title:

Digital Forensics

HTTP Link:

<http://catalog.ferris.edu/courses/HSCJ210/>

Course Length:

This 3 hour course consists of 45 hours of instruction over 7.5 weeks.

Course Description:

Students survey the role of computer technology in digital forensics and the characteristics of an incidence response plan and its implementation. Student will utilize several digital forensic tools and techniques for surveillance, gathering evidence, and reconstructing crime scenes.

Course Learning Objective:

1. Identify and describe the role of computer technology in computer forensics
2. Identify and describe the characteristics and implementation of an incident response plan
3. Identify and describe the capabilities of digital forensics tools
4. Describe and utilize digital forensics tools for surveillance, gathering evidence and crime scene reconstruction

Major Topics:

1. The role of computer technology in digital forensics
 - 1.1 Overview of computer technology
 - 1.2 The use of computer technology in computer crime
 - 1.3 Crime scene procedures
2. Incidence response plan
 - 2.1 Components
 - 2.2 Implementation techniques and procedures
 - 2.3 Utilization
3. Digital forensic tools
 - 3.1 Types and capabilities
 - 3.2 Procedures and protocols
 - 3.3 Utilization

4. Surveillance, gathering evidence, crime scene reconstruction
- 4.1 Integrating digital tools into the investigation process
- 4.2 What constitutes evidence
- 4.3 Preserving evidence

Method of Instruction:

Course is delivered in a mixed delivery format (in person and online instruction) consisting of:

1. Lectures
2. Individual and team hands-on exercises/demonstrations
3. Individual and team projects
4. Case study review and analysis
5. Individual online research and assignments







Evaluation Methods:

1. Weekly Quizzes
2. Weekly Assignments
3. Comprehensive Final
4. Mock Trial Analysis and Prep
5. Participation

Student Enrollment

Current Year: 55

Past Years: 56

 Delete	 Print	 Edit	 Enter New Course	 Next Item	 Previous Item
--	---	--	--	---	---



Information Assurance Courseware Evaluation Program Course Information for Ferris State University

This Course Is Currently Being Taught:

Yes

Course Designator/Course Number:

HSCJ 315

Course Title:

Advanced Digital Forensics

HTTP Link:

<http://catalog.ferris.edu/courses/HSCJ315/>

Course Length:

This 3 hour course consists of 45 hours of instruction over 7.5 weeks.

Course Description:

Students explore advanced digital forensic techniques and develop skills to deal with situations requiring a sophisticated response. Emerging and next generation computer technologies and threats as well as proactive security measures and threat prevention will also be investigated. Students will utilize several digital forensic tools and techniques for surveillance, gathering evidence, and-or crime scene reconstruction for incidence processing.

Course Learning Objective:

1. Identify and describe emerging computer technologies and the threats they pose
2. Develop skills for creating proactive security measures
3. Describe and utilize digital forensic tools for surveillance, gathering evidence and crime scene reconstruction
4. Develop skills for incident response

Major Topics:

1. Emerging computer technologies and threats
 - 1.1 Research techniques
 - 1.2 The use of computer technology in computer crime
 - 1.3 Threats to security
2. Proactive security measures
 - 2.1 Metrics and vulnerabilities
 - 2.2 Risk analysis
 - 2.3 Risk response
3. Surveillance, gathering evidence, crime scene reconstruction
 - 3.1 Use of non-invasive forensic analysis tools

- 3.2 Procedures and protocols
- 3.3 Chain of possession
- 4. Incident processing
 - 4.1 Acquisition of digital evidence
 - 4.2 Preserving digital evidence
 - 4.3 Analysis of digital evidence
 - 4.4 Developing a case and presenting digital evidence

Method of Instruction:

Course is delivered in a mixed delivery format (in person and online instruction) consisting of:

1. Lectures
2. Individual and team hands-on exercises/demonstrations
3. Individual and team projects
4. Case study review and analysis
5. Individual online research and assignments

Evaluation Methods:

1. Weekly Quizzes
2. Weekly Assignments
3. Comprehensive Final
4. Mock Trial Analysis and Prep
5. Participation

Student Enrollment

Current Year: 45

Past Years: 41

 Delete	 Print	 Edit	 Enter New Course	 Next Item	 Previous Item
--	---	--	--	---	---



Information Assurance Courseware Evaluation Program Course Information for Ferris State University

This Course Is Currently Being Taught:

Yes

Course Designator/Course Number:

HSCJ 317

Course Title:

Fraud Examination

HTTP Link:

<http://catalog.ferris.edu/courses/HSCJ317/>

Course Length:

This 3 hour course consists of 45 hours of instruction over 7.5 weeks.

Course Description:

Students will examine the fundamental reasons of why people commit fraud. Participants will investigate and explore how opportunity, pressures and rationalization are linked together to foster an atmosphere that can allow fraud to occur. Additionally, students will learn basic examination techniques for discovering fraud and more importantly, how to deter fraud from taking place.

Course Learning Objective:

Identify and describe various forms of employee and financial statement fraud.
Identify and describe procedures, checks and balances and other methods of preventing fraud.
Investigate methods of collection and handling evidence including interviewing techniques, auditing books.
Identify and describe corruption in the form of conflict of interest and bribery in the corporate environment.

Major Topics:

Types of financial fraud
Use of technology to investigate financial fraud
methods of collecting and handling electronic evidence.

Method of Instruction:

Lecture
Presentations
Case studies


Evaluation Methods:

Assessment
Research paper
Case studies

Student Enrollment

Current Year: 40

Past Years: 40

 Delete	 Print	 Edit	 Enter New Course	 Next Item	 Previous Item
--	---	--	--	---	---



Information Assurance Courseware Evaluation Program Course Information for Ferris State University

This Course Is Currently Being Taught:

Yes

Course Designator/Course Number:

ISIN 200

Course Title:

All Things Digital

HTTP Link:

<http://catalog.ferris.edu/courses/ISIN200/>

Course Length:

This 3 hour course consists of 45 hours of instruction over 7.5 weeks.

Course Description:

Students investigate various digital devices including computers, cameras, surveillance equipment, and small devices and how to utilize them to advance security objectives. Students also work with various forms of media to understand the capabilities of each. Communication methods and networking are also explored.

Course Learning Objective:

1. Identify and describe various digital devices and storage formats.
2. Develop skills to utilize digital devices for information gathering dissemination.
3. Assess the abilities of digital devices in criminal and security roles, and potential evidence gathering techniques.
4. Theorize ways digital devices could be used for security and criminal activity.

Major Topics:

1. What is digital?
 - 1.1 Introduction to binary
 - 1.2 Introduction to hexadecimal
 - 1.3 Introduction to computer components
 - 1.4 Introduction to media storage devices
 - 1.5 Hard Drive – Low Level and high level formats
 - 1.6 CD/ROMs and DVDs
 - 1.7 Thumb Drives
2. Introduction to Tools for looking at things in binary and/or hexadecimal
 - 2.1 Hard drive format options
 - 2.2 Storage Devices

- 2.3 Software for viewing files in hex & binary
- 3. Introduction to image media
 - 3.1 Still image formats (JPEG, GIF, BMP, others)
 - 3.2 Camera Output formats
 - 3.3 Digital camera options & features
 - 3.4 Image editing/viewing software
 - 3.5 Motion picture formats (MP4, Quicktime, DVD)
- 4. Introduction to audio media
 - 4.1 Compression
 - 4.2 Sampling
 - 4.3 Lossless
 - 4.4 Lossful
 - 4.5 WAV
 - 4.6 AU
 - 4.7 AIFF
 - 4.8 MP3
- 5. Introduction to text media
 - 5.1 Word
 - 5.2 Excel
 - 5.3 Powerpoint
 - 5.4 HTML
 - 5.5 XML
 - 5.6 Encryption

Method of Instruction:

Course is delivered in a mixed delivery format (in person and online instruction) consisting of:

1. lectures
2. individual and team hands-on exercises/demonstrations
3. individual and team projects
5. individual online work and research







Evaluation Methods:

1. Scheduled quizzes
2. Final Exam
3. Group projects and reports
4. Current topic research, presentations and discussion contributions

Student Enrollment

Current Year: 48

Past Years: 41

 Delete	 Print	 Edit	 Enter New Course	 Next Item	 Previous Item
--	---	--	--	---	---



Information Assurance Courseware Evaluation Program Course Information for Ferris State University

This Course Is Currently Being Taught:

Yes

Course Designator/Course Number:

ISIN 330

Course Title:

Org Crime-Gang-Terrorist Org

HTTP Link:

<http://catalog.ferris.edu/courses/ISIN330/>

Course Length:

This 3 hour course consists of 45 hours of instruction over 7.5 weeks.

Course Description:

Students investigate the history of significant organized crime, gangs and terrorist organizations and the techniques they utilize. Examination will include the culture and organization of contemporary organized crime, gangs and terrorist groups, as well as the threats they pose. Methods used to combat the work of these organizations will be analyzed.

Course Learning Objective:

Provide students with a conceptual framework for studying the problem of organized crime, gangs and terrorism.

Provide students a historical background on organized crime, gang and terrorist organizations.

Identify and describe organized crime, gang and terrorist organizations and their culture.

Develop skills for evaluating the effectiveness of the techniques used by organized crime, gang and terrorist organizations.

Analyze the methods used to combat organized crime, gangs and terrorism.

Theorize on ways to mitigate the impact of organized crime, gang and terrorist organizations.

Major Topics:

Evaluate electronic methods used by terrorists and organized crime.

Identify skills to investigate terrorist and organized crime activity in a digital environment

Identify methods to combat organized crime, gangs and terrorism.

Method of Instruction:

Lecture
Presentations
On-line learning







Evaluation Methods:

Assessments
Groups Presentations
Essays

Student Enrollment

Current Year: 20

Past Years: 20

 Delete	 Print	 Edit	 Enter New Course	 Next Item	 Previous Item
--	---	--	--	---	---



Information Assurance Courseware Evaluation Program Course Information for Ferris State University

This Course Is Currently Being Taught:

Yes

Course Designator/Course Number:

ISIN 429

Course Title:

Legal-Ethical Issues Infor Sec

HTTP Link:

<http://catalog.ferris.edu/courses/ISIN429/>

Course Length:

This 3 hour course consists of 45 hours of instruction over 7.5 weeks.

Course Description:

This course is intended to investigate the legal and ethical issues in Information Security. Ethical practices, privacy, copyright and licensing issues are researched. This issues dealing with proprietary and personal information, as well as electronic technologies will be studied. An understanding of current and future impact on information systems and management strategies will be explored.

Course Learning Objective:







1. Analyze the moral and legal dilemmas that arise in the areas of free speech, intellectual property, privacy, licensing, and security
2. Develop an understanding of the ever-increasing global nature of IT ethics and how ethical/unethical decisions impact the global community
3. Gain a better understanding of various generational differences that people possess based on the historical events that occurred during their childhood and how those differences shape individual values as a basis for personal decision making
4. Investigate and provide practice in applying a code of ethics and professional conduct to actual or hypothetical case studies

Major Topics:

1. Legal and moral issues
 - 1.1 Free speech
 - 1.2 Intellectual property
 - 1.3 Privacy
 - 1.4 Security
 - 1.5 Licensing

- 2. The impact of ethics
 - 2.1 Global issues
 - 2.2 Decision making
 - 2.3 Relationships
 - 2.4 Costs
- 3. Personal values
 - 3.1 Education
 - 3.2 Culture
 - 3.3 Generation types
- 4. Ethical codes
 - 4.1 Survey and investigation
 - 4.2 Developing a code of ethics
 - 4.3 Case studies

Method of Instruction:**Evaluation Methods:****Student Enrollment****Current Year:** 25**Past Years:** 17

 Delete	 Print	 Edit	 Enter New Course	 Next Item	 Previous Item
--	---	--	--	---	---



**Information Assurance
Courseware Evaluation Program
Course Information
for
Ferris State University**

This Course Is Currently Being Taught:

Yes

Course Designator/Course Number:

ISYS 200

Course Title:

Database Design-Implementation

HTTP Link:

<http://catalog.ferris.edu/courses/ISYS200/>

Course Length:

This 3 hour course consists of 45 hours of instruction over 15 weeks.

Course Description:

Introduces database concepts, design methodologies, and implementation procedures. Stresses the importance of sound database design to insure data integrity and flexibility. Common data structures, normalization techniques, integrity constraints, security features, query and report facilities are discussed. One or more popular commercial database management systems will be used to implement the designs.

Course Learning Objective:

1. Understand the basic concepts of relational databases.
2. Create tables, define data types, create data input rules and define relationships between tables.
3. Use automated query, form, report, and web publishing tools in Access.
4. Manually create multiple query types in Access that include joins and intermediate selection criteria.
5. Manually create forms in Access from tables and queries that include subforms.
6. Manually create reports in Access from tables and queries that include subreports.
7. Demonstrate the ability to integrate tables, queries, reports, and web publishing for use in database management.

Major Topics:

1. Introduction to relational data base concepts
2. Creating a Database
3. Building a Database and Defining Table Relationships
4. Maintaining and Querying a Database
5. Creating Forms and Reports

6. Creating Advanced Queries and Enhancing Table Design
7. Using Form Tools and Creating Custom Forms
8. Creating Custom Reports
9. Sharing, Integrating, and Analyzing Data
10. Using Action Queries and Advanced Table Relationships
11. Automating Tasks with Macros
12. Using and Writing Visual Basic for Applications Code
13. Managing and Securing a Database Additional Cases
14. Relational Databases and Database Design

Method of Instruction:

1. Lectures
2. In-class examples and discussion
3. In class exercises
4. Chapter tutorials and cases

Evaluation Methods:

1. Reading and cases
2. Chapter quizzes
3. Database projects
4. Quizzes and exams

Student Enrollment

Current Year: 275

Past Years: 280

 Delete	 Print	 Edit	 Enter New Course	 Next Item	 Previous Item
--	---	--	--	---	---



Information Assurance Courseware Evaluation Program Course Information for Ferris State University

This Course Is Currently Being Taught:

Yes

Course Designator/Course Number:

ISYS 325

Course Title:

Networking Essentials

HTTP Link:

<http://catalog.ferris.edu/courses/ISYS325/>

Course Length:

This 3 hour course consists of 45 hours of instruction over 15 weeks.

Course Description:

A study of networking hardware, transmission media, communication protocols, the Open System Interconnection (OSI), and distributed networking/processing. The equipment, techniques, and software utilized in networks are presented. Appropriate terminology and concepts utilized in networks are introduced. Lecture workshop experience with designing, planning, installing, and maintaining a Local Area Network.

Course Learning Objective:

1. Understand networking hardware, transmission media, the Open System Interconnection model (OSI), and distributed networking/processing for both LANs and WANs including the equipment, techniques, and software utilized in networks.
2. Demonstrate the ability to design, implement, and troubleshoot small peer-to-peer and client/server networks, including installing Windows and any necessary client software.
3. Demonstrate proper documentation of a network.
4. Compare and contrast the various network protocols.
5. Analyze a company's needs/benefits for networking and problems inherent in the non-planned networking environment.
6. Compare and contrast the characteristics of PANs, LANs, MANs, WANs, and VLANs, and identify the hardware and software of each and when each is appropriate.
7. Understand the various types of wireless communications, the security issues surrounding wireless communications, and when wireless is appropriate.
8. Function in a team environment
9. Identify and compare future trends of networking.

Major Topics:

1. Introduction and hardware

- 1.1 Learning how to use WebCT components
- 1.2 Definitions of LAN, PAN, SAN, NAS, MAN, WAN, and VLAN
- 1.3 What is a local area network? The physical and logical components which includes topology, various cables types, network interface cards (NICs)
- 1.4 Difference between a peer-to-peer and client/server network. (hardware and software required to create both types of LANs)
- 1.5 What is a server and how is it different than a work station
- 1.6 What are the major NOSs in a client/server network
- 1.7 Installing Windows and understanding what role Windows plays in networking the computer\
- 1.8 Touring the College of Business networking closets and documenting the design
- 1.9 Installing Visio
- 1.10 Introduction to wireless

2. Software

- 2.1 The OSI model
- 2.2 The protocols, Appletalk, IPX/SPX, TCP/IP, NetBeui, NetBIOS
- 2.3 Wireless networks
- 2.4 network architectures
- 2.5 Peer-to-peer networks and documentation
- 2.6 Client/server networks and documentation

Part 3: Advanced networks, WAN, MAN

- 1.1 Hardware and software for a MAN, WAN
- 1.2 Difference between bridge, router, switch, hub, repeater, gateway, brouter
- 1.3 Issues related to maintaining a network

Method of Instruction:

1. Lectures
2. In-class examples and discussion
3. Web page access
4. Hands-on demonstrations
5. Hands-on team assignments
6. Final team project


Evaluation Methods:

1. Team evaluations and presentations
2. Quizzes and exams
3. Producing a document using drawing software such as Visio,
4. Final team Project (Develop a networking solution for a company)
5. Individual paper on a networking topic not covered in the class

Student Enrollment

Current Year: 45

Past Years: 43

 Delete	 Print	 Edit	 Enter New Course	 Next Item	 Previous Item
--	---	--	--	---	---



Information Assurance Courseware Evaluation Program Course Information for Ferris State University

This Course Is Currently Being Taught:

Yes

Course Designator/Course Number:

ISYS 371

Course Title:

Adv Database Design-Implementation

HTTP Link:

<http://catalog.ferris.edu/courses/ISYS371/>

Course Length:

This 3 hour course consists of 45 hours of instruction over 7.5 weeks.

Course Description:

Emphasis is placed on Entity-Relationships and Relational models, data definition languages, and manipulation languages. Structured Query Language (SQL) is used to develop database objects such as databases, logs, tables, indexes, views, constraints, defaults, roles, rules, stored procedures, and triggers. Database design is reviewed. Application development and modeling tools are discussed. Projects requiring the development of integrated databases are assigned.

Course Learning Objective:

1. Understand data structures
2. Be able to Design a database
3. Understand common data constructs
4. Understand and perform the normalization of databases
5. Understand data models
6. Understand and use indexes
7. Understand and be able to maintain data integrity
8. Understand and use SQL
9. Understand XML

Major Topics:

1. Orientation/DB History/SQL Server
2. Client/Server & Distributed Processing
3. Database Architecture/
4. What is SQL Server
5. Understanding Database objects
6. Entity-Relationship Diagrams

7. Normalization
8. DB Objects and SQL DML Exercise
9. Stored Procedures
- 10 Stored Procedures and Triggers

Method of Instruction:

1. Lectures
2. In-class examples and discussion
3. In class exercises
4. Web page access







Evaluation Methods:

1. Quizzes
2. Article Reviews
3. Tests
4. Group Project
5. Individual Project

Student Enrollment

Current Year: 45

Past Years: 53

 Delete	 Print	 Edit	 Enter New Course	 Next Item	 Previous Item
--	---	--	--	---	---



Information Assurance Courseware Evaluation Program Course Information for Ferris State University

This Course Is Currently Being Taught:

Yes

Course Designator/Course Number:

ISYS 411

Course Title:

Project Management

HTTP Link:

<http://catalog.ferris.edu/courses/ISYS411/>

Course Length:

This 3 hour course consists of 45 hours of instruction over 15 weeks.

Course Description:

An in-depth study of project management techniques currently employed for business and information systems projects. Topical areas will include project organization, planning administration control and leadership. The need for accurate estimating, scheduling, communicating and reporting will be stressed through the use of several cases/projects.

Course Learning Objective:

The student will examine project management knowledge areas and apply that knowledge in the preparation of project documents, deliverables, and team work.

The student will evaluate project management best practices and assess their effectiveness and value through practice assignments and collaborative discussion.

The student will work within a team to develop a comprehensive project plan focused on managing a successful project throughout its life cycle.

The student will apply the Project Management Institute's Code of Ethics and Professional Responsibility and apply the code to various scenarios common in project management.

The student will evaluate their need to further develop interpersonal skills such as communication, conflict management, leadership and team building through practice scenarios with other students.

Major Topics:

Project Management Life Cycle

Project Management Knowledge Areas: Integration, Scope, Time, Cost, Quality, Communication, Procurement, Human Resources

Method of Instruction:

Lecture
Presentation







Evaluation Methods:

Discussion
Group Project
Assessments

Student Enrollment

Current Year: 80

Past Years: 80

 Delete	 Print	 Edit	 Enter New Course	 Next Item	 Previous Item
--	---	--	--	---	---



Information Assurance Courseware Evaluation Program Course Information for Ferris State University

This Course Is Currently Being Taught:

Yes

Course Designator/Course Number:

MISM 610

Course Title:

Database Management and Administration

HTTP Link:

<http://catalog.ferris.edu/courses/MISM610/>

Course Length:

This 3 hour course consists of 45 hours of instruction over 7.5 weeks.

Course Description:

Students investigate progressive database management and administration principles. Topics include design, implementation, and management techniques. Students utilize data definition and manipulation languages on leading database platforms. Emerging trends in database technology are also scrutinized.

Course Learning Objective:

Demonstrate an understanding of database fundamentals by being able to critique the validity of various database solutions.

Analyze, compare and contrast major products, vendors and supporting database technologies.

Formalize and construct normalized database structures.

Recognize the relevant issues surrounding database structures, support and operational considerations.

Assess implications of change, emerging technologies and organizational needs.

Analyze security requirements and techniques, and construct an appropriate model that satisfies these requirements.

Develop systematic backup and recovery strategies to support organizational requirements.

Major Topics:

Database design.

Database security.

SQL queries.

Method of Instruction:

Lecture
Presentation
Hands-on

Evaluation Methods:

Assessments
Projects
Group work

Student Enrollment

Current Year: 40

Past Years: 40



Information Assurance Courseware Evaluation Program Course Information for Ferris State University

This Course Is Currently Being Taught:

Yes

Course Designator/Course Number:

MISM 629

Course Title:

Legal and Ethical Issues in Business

HTTP Link:

<http://catalog.ferris.edu/courses/MISM629/>

Course Length:

This 3 hour course consists of 45 hours of instruction over 7.5 weeks.

Course Description:

This course will investigate legal and ethical issues including ethical practices, privacy, copyright and licensing. Issues dealing with proprietary and personal information, as well as electronic technologies will be studied. An understanding of current and future impact on information systems corporate liability and management strategies will be explored.

Course Learning Objective:

Identify the source of ethics and how they plan a role in law making.

Understand the origin of laws and how they came into existence in the United States.

Understand what personal property rights and laws are and how they affect business and personal life in the United States

Identify and describe key issues with surveillance, both legal and illegal and from both the digital and physical realm.

Identify and describe both "white" and "black" hacking techniques.

Identify and explain the role of government regulations in restricting business and personal activity.

Understand the implications of internal laws in regards to digital surveillance and other online activity.

Major Topics:

Overview of lawmaking.

Laws, regulations and issues related to intellectual property rights.

Laws, regulations and issues related to malicious and ethical hacking.

Laws, regulations and issues related to digital surveillance.

Laws, regulations and issues regarding malicious hacking and security breaches.

Method of Instruction:

Lecture
Presentation
Case Studies

Evaluation Methods:

Research Paper
Assessment
Discussion
Group Work

Student Enrollment

Current Year: 40

Past Years: 40

 Delete	 Print	 Edit	 Enter New Course	 Next Item	 Previous Item
--	---	--	--	---	---



Information Assurance Courseware Evaluation Program Course Information for Ferris State University

This Course Is Currently Being Taught:

Yes

Course Designator/Course Number:

MISM 661

Course Title:

Principles of Information Security Management

HTTP Link:

<http://catalog.ferris.edu/courses/MISM661/>

Course Length:

This 3 hour course consists of 45 hours of instruction over 7.5 weeks.

Course Description:

Students investigate concepts and methodologies of information security and the Information Security Lifecycle (Protection). Topics include information security administration and Security+ and CISSP.

Course Learning Objective:

- Define and describe the concept of information security.
- Explain the difference between information security strategic and tactical goals and plans
- Examine the information security lifecycle from initiation through closing.
- Learn to produce information security policies and procedures.
- Recognize the role of risk assessment in information security.
- Examine the DOD requirements for information assurance accreditation and certification
- Learn to build an information security education and training programs
- Summarize effective management skills required for information security management.
- Examine the Information Security Ethics and Professional Responsibility
- Assess your personal information security management goals.

Major Topics:

Introduction to the concepts of information security
DIACAP - Department of Defense Information Assurance Certification and Accreditation Process
Security Knowledge Domains including access controls, physical security, operational security, physical security, security attacks and countermeasures.
Developing information security policies and programs
Examining information security models
Security legal and ethical issues

Method of Instruction:

Online Lectures and Presentations
Classroom Lectures, Presentations and Activities

Evaluation Methods:

Discussion Forum
Individual Assignments
Final Exam
Group Work

Student Enrollment

Current Year: 50

Past Years: 50

 Delete	 Print	 Edit	 Enter New Course	 Next Item	 Previous Item
--	---	--	--	---	---



Information Assurance Courseware Evaluation Program Course Information for Ferris State University

This Course Is Currently Being Taught:

Yes

Course Designator/Course Number:

MISM 662

Course Title:

Advanced Network Security

HTTP Link:

<http://catalog.ferris.edu/courses/MISM662/>

Course Length:

This 3 hour course consists of 45 hours of instruction over 7.5 weeks.

Course Description:

Students investigate concepts and methodologies of incidence response, cyber forensics (acquisition, preservation, analysis, and presentation of evidence) and the information security lifecycle. Topics include: cyber laws, cyber crimes, incidence response, pre-incident preparation, detection, notification, initial response, strategic decisions, response, recovery, and reporting.

Course Learning Objective:

1. Research the purposes of a network penetration test and testing options.
2. Synthesize network penetration testing knowledge and formulate network penetration testing plans for various scenarios.
3. Execute a network penetration test and interpret the results.
4. Recommend and implement preventive, defensive, and corrective measures based on network penetration testing results.

Major Topics:

Network Penetration Testing
Vulnerability Assessments
Technology tools for penetration testing

Method of Instruction:

Lecture
Hands-on





Evaluation Methods:

Assessment
Individual Assignment
Group projects

Student Enrollment

Current Year: 40

Past Years: 40

 Delete	 Print	 Edit	 Enter New Course	 Next Item	 Previous Item
--	---	--	--	---	---



Information Assurance Courseware Evaluation Program Course Information for Ferris State University

This Course Is Currently Being Taught:

Yes

Course Designator/Course Number:

MISM 665

Course Title:

Management Information Systems

HTTP Link:

<http://catalog.ferris.edu/courses/MISM665/>

Course Length:

This 3 hour course consists of 45 hours of instruction over 7.5 weeks.

Course Description:

Students develop and understand the strategic framework in which contemporary organizations evaluate, develop and utilize management information systems. The student will be introduced to the information system life cycle, fundamental structures and tools used in system development, and an understanding of current and future trends in information system technology through hands-on and theoretical practice.

Course Learning Objective:

Understand organizational structure and culture
Examine key concepts of project management
Evaluate vendor management techniques and challenges
Assess the role of IT in organizations
Understand the key aspects of system analysis and design

Major Topics:

Information System Management concepts
Successfully implements projects in a business environment
Managing vendors to accomplish organizational goals
Examining the various types of IT structures in organizations
System analysis and design principles.

Method of Instruction:







Lecture
Presentation
Discussion

Evaluation Methods:

Assessments
Individual assignments
Discussion
Group work

Student Enrollment

Current Year: 40
Past Years: 40

 Delete	 Print	 Edit	 Enter New Course	 Next Item	 Previous Item
--	---	--	--	---	---



Information Assurance Courseware Evaluation Program Course Information for Ferris State University

This Course Is Currently Being Taught:

Yes

Course Designator/Course Number:

MISM 670

Course Title:

Network Management and Design

HTTP Link:

<http://catalog.ferris.edu/courses/MISM670/>

Course Length:

This 3 hour course consists of 45 hours of instruction over 7.5 weeks.

Course Description:

Students will examine the basic components of Local Area Networks including topologies, protocols, and wiring schemes. Operating environments explored will be both peer to peer and at least one server based network. Once exposed to managing these environments, the student will employ their analytical skills in determining the strengths and weaknesses of each of the environments.

Course Learning Objective:

- Understand various network topologies and protocols
- Evaluate the OSI network model
- Assess network hardware, software, and networking components
- Examine various network operating systems
- Assess network security issues and solutions
- Examine network administration tasks

Major Topics:

- Network topologies and protocols
- OSI model
- Network hardware, software, and components
- Network operation systems
- Network security
- Network administration

Method of Instruction:

Lecture
Presentation
Hands-on activities

Evaluation Methods:

Assessments
Individual assignments
Individual project
Group project

Student Enrollment

Current Year: 40

Past Years: 40

 Delete	 Print	 Edit	 Enter New Course	 Next Item	 Previous Item
--	---	--	--	---	---



Information Assurance Courseware Evaluation Program Course Information for Ferris State University

This Course Is Currently Being Taught:

Yes

Course Designator/Course Number:

MISM 740

Course Title:

Business Intelligence

HTTP Link:

<http://catalog.ferris.edu/courses/MISM740/>

Course Length:

This 3 hour course consists of 45 hours of instruction over 7 weeks.

Course Description:

An investigation of business intelligence and evaluation of analytical data used in strategic decision making. Topics include tracking, managing and understanding organized data, as well as identifying and measuring performance metrics. Includes applied decision making using appropriate tools and techniques. Decision support systems, data warehousing and emerging topics are explored.

Course Learning Objective:

- Examine the history and purpose of Business Intelligence including Executive and Decision Support Systems.
- Define and describe the Business Intelligence methodology.
- Define and describe the elements of Data Warehousing.
- Explain data extraction, transformation and load (ETL) processes of Data Warehousing.
- Examine real-time data warehousing.
- Define and describe the use of Business Analytics.
- Explain the concepts of online analytical processing (OLAP), data visualization, and data mining.
- Explore web intelligence and web analytics.

Define and describe data mining and its uses in businesses.

Understand how Business Intelligence supports Business Performance Management

Explore the major issues in implementing Business Intelligence

Examine the Business Intelligence components: architecture, databases, data warehouses, performance management, and reporting & querying.

Utilize hands on exercises in Business Analytics, Data Visualization and Data Mining technologies.

Explore the use of Business Intelligence technology tools.

Major Topics:

History of Business Intelligence
Data warehousing
Data mining
Web mining
Real-time analysis
Business analytics

Method of Instruction:

Lecture
Presentation

Evaluation Methods:

Assessments
Individual assignment
Group assignment
Discussion

Student Enrollment

Current Year: 40

Past Years: 40

Delete	Print	Edit	Enter New Course	Next Item	Previous Item
------------------------	-----------------------	----------------------	----------------------------------	---------------------------	-------------------------------



Information Assurance Courseware Evaluation Program Course Information for Ferris State University

This Course Is Currently Being Taught:

Yes

Course Designator/Course Number:

MMBA 640

Course Title:

Project Management

HTTP Link:

<http://catalog.ferris.edu/catalog0607/courses/MMBA640/>

Course Length:

This 3 hour course consists of 45 hours of instruction over 7.5 weeks.

Course Description:

Examines the role of project management and its use in business and organizations. Each of the following constituent elements for successful project management is included in the course: defining a project, working with project teams, performing projects budgeting, performing a work breakdown analysis, creating a project schedule, and performing project monitoring and evaluation.

Course Learning Objective:

The students will understand the concept of a project lifecycle.

The student will become familiar with the project management knowledge areas including project integration, human resource, project time management, project costing, communication, stakeholder management, procurement management and risk management.

The student will evaluate the role of the Project Management Office (PMO)

Major Topics:

Overview of Project Management

Project Office

Project Integration

Human Aspects

Project Scheduling/Time Management

Project Costing

Risk Management

Quality

Third Parties

Communications

Project Reviews
Politics

Method of Instruction:

Lecture
Presentation
Case Studies

Evaluation Methods:

Assessments
Individual Assignment
Group Work
Discussion

Student Enrollment

Current Year: 40

Past Years: 40

 Delete	 Print	 Edit	 Enter New Course	 Next Item	 Previous Item
--	---	--	--	---	---



Information Assurance Courseware Evaluation Program Course Information for Ferris State University

This Course Is Currently Being Taught:

Yes

Course Designator/Course Number:

STQM 342

Course Title:

Data Mining Tools

HTTP Link:

<http://catalog.ferris.edu/courses/STQM342/>

Course Length:

This 3 hour course consists of 45 hours of instruction over 15 weeks.

Course Description:

Principles and tools for extracting information and creating knowledge from large databases through application of software. Tools include k-means clustering, classification, association, and others. Software applications to large data sets (e.g. Excel, Access, SQL Server, SPSS).

Course Learning Objective:

By the end of this course, the student should be able to:

1. Define data mining, data warehousing, and organizational needs and articulate ways in which these three are inter-related within an organizational context.
2. Identify organizational needs amenable to data mining and communicate ways in which data mining meets those needs.
3. Describe the role of data mining and data miners within an organization, particularly as related to organizational needs assessment, information needs assessment, data warehousing, data extraction, data preparation, pattern recognition, and reporting.
4. Express basic approaches to data storage, retrieval, and preparation pursuant to data mining applications.
5. Identify and apply basic approaches and pattern detection tools utilized in data mining and ways of assessing their effectiveness.
6. Articulate the support and operational roles of software to data mining.
7. Express ways in which data mining serves particular organizational needs in various areas of application, including business, marketing, education, healthcare, criminal justice, and government.

Major Topics:

Data mining techniques
Data mining tools

Method of Instruction:

Lecture
Presentations
Software

Evaluation Methods:

Quizzes
Tests






Student Enrollment

Current Year: 75

Past Years: 75

B. CNSS Standard NTSTISSI 4011

a. Course Mapping Details

 Print	 Collapse All	 Expand All	 Previous Page	 Next Page
---	--	--	---	--

Welcome Barbara Ciaramitaro, it is Monday, August 16, 2010 at 03:32:56 PM
You are currently viewing a report for NSTISSI 4011 sorted by element.

▼ A. COMMUNICATIONS BASICS (Awareness Level)

▼ Instructional Content

▼ Describe vehicles of transmission

▼ NO SUB-CATEGORY

ISYS 325,MISM 670

▼ Introduce the evolution of modern communications systems

▼ NO SUB-CATEGORY

ISYS 325,MISM 670

▼ (1) Topical Content

▼ (a) Historical vs Current Methodology

▼ NO SUB-CATEGORY

ISYS 325

▼ (b) Capabilities and limitations of various communications systems

▼ dedicated line

ISYS 325,MISM 670

▼ digital vs analog

ISYS 325,MISM 670

▼ line of sight

ISYS 325,MISM 670

▼ microwave

ISYS 325,MISM 670

▼ public switched network

ISYS 325,MISM 670

▼ radio frequency (e.g., bandwidth)

ISYS 325,MISM 670

▼ satellite

ISYS 325,MISM 670

▼* asynchronous vs synchronous

ISYS 325,MISM 670

▼ B. AUTOMATED INFORMATION SYSTEMS (AIS) BASICS (Awareness Level)

▼ Instructional Content

▼ Describe an AIS environment

▼ NO SUB-CATEGORY

ISYS 325,MISM 670

▼ Provide language of an AIS

▼ NO SUB-CATEGORY

ISYS 325,MISM 670

▼ **Providing an overview of hardware, software, firmware components of an AIS, to integrate into information systems security aspects/behaviors discussed later**

- ▼ NO SUB-CATEGORY
ISYS 325,MISM 670

▼ **(1) Topical Content**

▼ **(a) Historical vs Current Technology**

- ▼ NO SUB-CATEGORY
ISYS 325,HSCJ 315

▼ **(b) Hardware**

- ▼ components (e.g., input, output, central processing unit (CPU))
ISYS 325,MISM 670,HSCJ 315
- ▼ distributed vs stand-alone
ISYS 325,MISM 670,HSCJ 315
- ▼ micro, mini, mainframe processors
ISYS 325,MISM 670,HSCJ 315
- ▼ storage devices
ISYS 325,MISM 670,HSCJ 315

▼ **(c) Software**

- ▼ applications
HSCJ 202,ISYS 325,MISM 670
- ▼ operating system
ISYS 325,MISM 670,HSCJ 315

▼ **(d) Memory**

- ▼ sequential
HSCJ 315
- ▼ volatile vs nonvolatile
HSCJ 315
- ▼* random
HSCJ 202,HSCJ 315

▼ **(e) Media**

- ▼ optical remanence
HSCJ 202,MISM 661
- ▼* magnetic remanence
HSCJ 202,MISM 661

▼ **(f) Networks**

- ▼ file servers
ISYS 325,MISM 670
- ▼ modems
ISYS 325,MISM 670
- ▼ sharing of data
ISYS 325,MISM 670
- ▼ sharing of devices
ISYS 325,MISM 670
- ▼ switching

ISYS 325,MISM 670

▼ topology

ISYS 325,MISM 670

▼* asynchronous vs synchronous

ISYS 325,MISM 670

▼ **C. SECURITY BASICS (Awareness Level)**

▼ **Instructional Content**

▼ **Using the Comprehensive Model of Information Systems Security (contained in the Annex to this instruction), introduce a comprehensive model of information systems security that addresses:**

▼ information states

HSCJ 202,MISM 661

▼ security measures

HSCJ 202,MISM 661

▼* critical characteristics of information

HSCJ 202,MISM 661

▼ **(1) Topical Content**

▼ **(a) INFOSEC Overview**

▼ critical information characteristics - confidentiality

HSCJ 202,MISM 661

▼ critical information characteristics - integrity

HSCJ 202,MISM 661

▼ information states - storage

HSCJ 202,HSCJ 210,MISM 661

▼ information states - transmission

HSCJ 202,MISM 670,MISM 661

▼ security countermeasures - policy, procedures and practices

HSCJ 202,HSCJ 210,MISM 661

▼ security countermeasures - technology

HSCJ 202,MISM 661

▼ threats

HSCJ 202,MISM 661

▼ vulnerabilities

HSCJ 202,MISM 661,MISM 662

▼* critical information characteristics - availability

HSCJ 202,MISM 661

▼* information states - processing

HSCJ 202,MISM 661

▼* security countermeasures - education, training and awareness

HSCJ 202,MISM 661

▼ **(b) Operations Security (OPSEC)**

▼ OPSEC process

HSCJ 202,MISM 661

▼ OPSEC surveys/OPSEC planning

HSCJ 202,MISM 661

- ▼ unclassified indicators
 - [HSCJ 202,MISM 661](#)
- ▼* INFOSEC and OPSEC interdependency
 - [HSCJ 202,MISM 661](#)
- ▼ **(c) Information Security**
 - ▼ policy
 - [HSCJ 202,MISM 661](#)
 - ▼ roles and responsibilities
 - [HSCJ 202,MISM 661](#)
 - ▼* application dependent guidance
 - [HSCJ 202,MISM 661](#)
- ▼ **(d) INFOSEC**
 - ▼ computer security - audit
 - [HSCJ 202,MISM 661](#)
 - ▼ computer security - identification and authentication
 - [HSCJ 202,MISM 661](#)
 - ▼ computer security - object reuse
 - [HSCJ 202](#)
 - ▼ cryptography - key management (to include electronic key)
 - [HSCJ 202,HSCJ 315,MISM 661](#)
 - ▼ cryptography - strength (e.g., complexity, secrecy, characteristics of the key)
 - [HSCJ 202,HSCJ 315,MISM 661](#)
 - ▼ emanations security
 - [HSCJ 202,MISM 661](#)
 - ▼ physical, personnel and administrative security
 - [HSCJ 202,MISM 661](#)
 - ▼ transmission security
 - [HSCJ 202,MISM 670](#)
 - ▼* computer security - access control
 - [HSCJ 202,MISM 661](#)
 - ▼* cryptography - encryption (e.g., point-to-point, network, link)
 - [HSCJ 202,HSCJ 315,MISM 661](#)
- ▼ **D. NSTISS BASICS (Awareness Level)**
 - ▼ **Instructional Content**
 - ▼ **Describe components (with examples to include: national policy, threats and vulnerabilities, countermeasures, risk management, systems lifecycle management, trust, modes of operation, roles of organizational units, facets of NSTISS**
 - ▼ NO SUB-CATEGORY
 - [HSCJ 202,ISIN 330,MISM 661](#)
- ▼ **(1) Topical Content**
 - ▼ **(a) National Policy and Guidance**
 - ▼ communications security
 - [HSCJ 202,MISM 670,MISM 661](#)
 - ▼ employee accountability for agency information

HSCJ 202,MISM 661

▼ protection of information

HSCJ 202,MISM 661

▼* AIS security

HSCJ 202,MISM 661

▼ **(b) Threats to and Vulnerabilities of Systems**

▼ major categories of threats (e.g., fraud, Hostile Intelligence Service (HOIS), malicious logic, hackers, environmental and technological hazards, disgruntled employees, careless employees, HUMINT, and monitoring)

HSCJ 202,MISM 661,MISM 662

▼ threat impact areas

HSCJ 202,MISM 661,MISM 662

▼* definition of terms (e.g., threats, vulnerabilities, risk)

HSCJ 202,MISM 661

▼ **(c) Legal Elements**

▼ evidence collection and preservation

HSCJ 202,HSCJ 210,ISIN 200,MISM 661

▼ fraud, waste and abuse

HSCJ 202,HSCJ 317,MISM 661

▼ investigative authorities

HSCJ 202,HSCJ 210,MISM 661

▼* criminal prosecution

HSCJ 202,HSCJ 210,HSCJ 315,MISM 661

▼ **(d) Countermeasures**

▼ assessments (e.g., surveys, inspections)

HSCJ 202,MISM 661,MISM 662

▼ cover and deception

HSCJ 202,HSCJ 315,MISM 661,MISM 662

▼ education, training, and awareness

HSCJ 202,MISM 661

▼ HUMINT

HSCJ 202,MISM 661

▼ monitoring (e.g., data, line)

HSCJ 202,MISM 661

▼ technical surveillance countermeasures

HSCJ 202,ISIN 200,MISM 661,MISM 662

▼ **(e) Concepts of Risk Management**

▼ cost/benefit analysis of controls

HSCJ 202,MISM 661

▼ implementation of cost-effective controls

HSCJ 202,MISM 661

▼ monitoring the efficiency and effectiveness of controls (e.g., unauthorized or inadvertent disclosure of information)

HSCJ 202,MISM 661

- ▼ threat and vulnerability assessment
 - [HSCJ 202,HSCJ 210,MISM 661,MISM 662](#)
- ▼ * consequences (e.g., corrective action, risk assessment)
 - [HSCJ 202,MISM 661](#)
- ▼ **(f) Concepts of System Life Cycle Management**
 - ▼ demonstration and validation (testing)
 - [HSCJ 202,MISM 661](#)
 - ▼ development
 - [HSCJ 202,MISM 661](#)
 - ▼ implementation
 - [HSCJ 202,MISM 661](#)
 - ▼ operations and maintenance (e.g., configuration management)
 - [HSCJ 202,MISM 661](#)
 - ▼ requirements definition (e.g., architecture)
 - [HSCJ 202,MISM 661](#)
 - ▼ security (e.g., certification and accreditation)
 - [HSCJ 202,MISM 661](#)
- ▼ **(g) Concepts of Trust**
 - ▼ mechanism
 - [HSCJ 202,MISM 661](#)
 - ▼ policy
 - [HSCJ 202,MISM 661](#)
 - ▼ * assurance
 - [HSCJ 202,MISM 661](#)
- ▼ **(h) Modes of Operation**
 - ▼ dedicated
 - [HSCJ 202,MISM 661](#)
 - ▼ multilevel
 - [HSCJ 202,MISM 661](#)
 - ▼ system-high
 - [HSCJ 202,MISM 661](#)
 - ▼ * compartmented/partitioned
 - [HSCJ 202,MISM 661](#)
- ▼ **(i) Roles of Various Organizational Personnel**
 - ▼ COMSEC custodian
 - [HSCJ 202,MISM 661](#)
 - ▼ end users
 - [HSCJ 202,MISM 661](#)
 - ▼ information resources management staff
 - [HSCJ 202,MISM 661](#)
 - ▼ INFOSEC Officer
 - [HSCJ 202,MISM 661](#)
 - ▼ OPSEC managers
 - [HSCJ 202,MISM 661](#)

- ▼ program or functional managers
 - HSCJ 202,MISM 661
- ▼ security office
 - HSCJ 202,MISM 661
- ▼ senior management
 - HSCJ 202,MISM 661
- ▼ system manager and system staff
 - HSCJ 202,MISM 661
- ▼ telecommunications office and staff
 - HSCJ 202,MISM 661
- ▼ * audit office
 - HSCJ 202,MISM 661
- ▼ **(j) Facets of NSTISS**
 - ▼ application of cryptographic systems
 - HSCJ 202,HSCJ 315,MISM 661
 - ▼ backup of data and files
 - HSCJ 202,MISM 661
 - ▼ protection against malicious logic
 - HSCJ 202,MISM 661
 - ▼ protection of areas
 - HSCJ 202,MISM 661
 - ▼ protection of data communications
 - HSCJ 202,MISM 661
 - ▼ protection of equipment
 - HSCJ 202,MISM 661
 - ▼ protection of files and data
 - HSCJ 202,MISM 661
 - ▼ protection of keying material
 - HSCJ 202,MISM 661
 - ▼ protection of magnetic storage media
 - HSCJ 202,MISM 661
 - ▼ protection of passwords
 - HSCJ 202,MISM 661
 - ▼ protection of voice communications
 - HSCJ 202,MISM 661
 - ▼ reporting security violations
 - HSCJ 202,HSCJ 210,MISM 661
 - ▼ transmission security countermeasures (e.g., callsigns, frequency, and pattern forewarning protection)
 - HSCJ 202,MISM 661
- ▼ **E. SYSTEM OPERATING ENVIRONMENT (Awareness Level)**
 - ▼ **Instructional Content**
 - ▼ **Describe Agency "control points" for purchase and maintenance of Agency AIS and telecommunications systems**
 - ▼ NO SUB-CATEGORY

HSCJ 202,MISM 661

▼ **Outline Agency specific AIS and telecommunications systems**

▼ NO SUB-CATEGORY

HSCJ 202,MISM 661

▼ **Review Agency AIS and telecommunications security policies**

▼ NO SUB-CATEGORY

HSCJ 202,MISM 661

▼ **(1) Topical Content**

▼ **(a) AIS**

▼ hardware

ISYS 325,MISM 670

▼ software

ISYS 325,MISM 670

▼ * firmware

ISYS 325,MISM 670

▼ **(b) Telecommunications Systems**

▼ software

HSCJ 202,MISM 670

▼ * hardware

HSCJ 202,MISM 670

▼ **(c) Agency Specific Security Policies**

▼ guidance

HSCJ 202,MISM 661

▼ points of contact

HSCJ 202,MISM 661

▼ roles and responsibilities

HSCJ 202,MISM 661

▼ **(d) Agency Specific AIS and Telecommunications Policies**

▼ references

HSCJ 202,MISM 661

▼ * points of contact

HSCJ 202,MISM 661

▼ **F. NSTISS PLANNING AND MANAGEMENT (Performance Level)**

▼ **Instructional Content**

▼ **Discuss practical performance measures employed in designing security measures and programs**

▼ NO SUB-CATEGORY

HSCJ 202,MISM 661

▼ **Introduce generic security planning guidelines/documents**

▼ NO SUB-CATEGORY

HSCJ 202,MISM 661

▼ **(1) Topical Content**

▼ **(a) Security Planning**

▼ NSTISS program budget

HSCJ 202,MISM 661

- ▼ NSTISS program evaluation
 - HSCJ 202,MISM 661
- ▼ NSTISS training (content and audience definition)
 - HSCJ 202,MISM 661
- ▼ * directives and procedures for NSTISS policy
 - HSCJ 202,MISM 661
- ▼ **(b) Risk Management**
 - ▼ corrective actions
 - HSCJ 202,HSCJ 210,MISM 661
 - ▼ information identification
 - HSCJ 202,MISM 661
 - ▼ risk analysis and/or vulnerability assessment components
 - HSCJ 202,MISM 661,MISM 662
 - ▼ risk analysis results evaluation
 - HSCJ 202,MISM 661
 - ▼ roles and responsibilities of all the players in the risk analysis process
 - HSCJ 202,MISM 661
 - ▼ * acceptance of risk (accreditation)
 - HSCJ 202,MISM 661
- ▼ **(c) Systems Life Cycle Management**
 - ▼ design review and systems test performance (ensure required safeguards are operationally adequate)
 - HSCJ 202,MISM 661
 - ▼ determination of security specifications
 - HSCJ 202,MISM 661
 - ▼ evaluation of sensitivity of the application based upon risk analysis
 - HSCJ 202,MISM 661
 - ▼ management control process (ensure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications and into significant modifications to existing applications)
 - HSCJ 202,MISM 661
 - ▼ systems certification and accreditation process
 - HSCJ 202,MISM 661
 - ▼ * acquisition
 - HSCJ 202,MISM 661
- ▼ **(d) Contingency Planning/Disaster Recovery**
 - ▼ contingency plan components
 - HSCJ 202,MISM 661
 - ▼ determination of backup requirements
 - HSCJ 202,MISM 661
 - ▼ development of plans for recovery actions after a disruptive event
 - HSCJ 202,MISM 661
 - ▼ development of procedures for off-site processing
 - HSCJ 202,MISM 661
 - ▼ emergency destruction procedures

HSCJ 202,MISM 661

- ▼ guidelines for determining critical and essential workload

HSCJ 202,MISM 661

- ▼ team member responsibilities in responding to an emergency situation

HSCJ 202,MISM 661

- ▼* agency response procedures and continuity of operations

HSCJ 202,MISM 661

▼G. NSTISS POLICIES AND PROCEDURES (Performance Level)

▼Instructional Content

- ▼List and describe: elements of vulnerability and threat that exist in an AIS/ telecommunications system with corresponding protection measures

- ▼NO SUB-CATEGORY

HSCJ 202,MISM 661,MISM 662

- ▼List and describe: specific technological, policy, and educational solutions for NSTISS

- ▼NO SUB-CATEGORY

HSCJ 202,MISM 661

▼(1) Topical Content

▼(a) Physical Security Measures

- ▼building construction

HSCJ 202,MISM 661

- ▼cabling

HSCJ 202,MISM 661

- ▼communications centers

HSCJ 202,MISM 661

- ▼environmental controls (humidity and air conditioning)

HSCJ 202,MISM 661

- ▼filtered power

HSCJ 202,MISM 661

- ▼fire safety controls

HSCJ 202,MISM 661

- ▼information systems centers

HSCJ 202,MISM 661

- ▼physical access control systems (key cards, locks and alarms)

HSCJ 202,MISM 661

- ▼power controls (regulator, uninterrupted power service (UPS), and emergency poweroff switch)

HSCJ 202,MISM 661

- ▼protected distributed systems

HSCJ 202,MISM 661

- ▼shielding

HSCJ 202,MISM 661

- ▼stand-alone systems and peripherals

HSCJ 202,MISM 661

- ▼ storage area controls
 - [HSCJ 202,MISM 661](#)
- ▼* alarms
 - [HSCJ 202,MISM 661](#)
- ▼ **(b) Personnel Security Practices and Procedures**
 - ▼ contractors
 - [HSCJ 202,MISM 661](#)
 - ▼ employee clearances
 - [HSCJ 202,MISM 661](#)
 - ▼ position sensitivity
 - [HSCJ 202,MISM 661](#)
 - ▼ security training and awareness (initial and refresher)
 - [HSCJ 202,MISM 661](#)
 - ▼ systems maintenance personnel
 - [HSCJ 202,MISM 661](#)
 - ▼* access authorization/verification (need-to-know)
 - [HSCJ 202,MISM 661](#)
- ▼ **(c) Software Security**
 - ▼ configuration management (change controls)
 - [HSCJ 202](#)
 - ▼ configuration management (documentation)
 - [HSCJ 202](#)
 - ▼ configuration management (programming standards and controls)
 - [HSCJ 202](#)
 - ▼ software security mechanisms to protect information (access privileges)
 - [HSCJ 202,MISM 661](#)
 - ▼ software security mechanisms to protect information (application security features)
 - [HSCJ 202](#)
 - ▼ software security mechanisms to protect information (audit trails and logging)
 - [HSCJ 202,MISM 661](#)
 - ▼ software security mechanisms to protect information (concept of least privilege)
 - [HSCJ 202,MISM 661](#)
 - ▼ software security mechanisms to protect information (identification and authentication)
 - [HSCJ 202,MISM 661](#)
 - ▼ software security mechanisms to protect information (internal labeling)
 - [HSCJ 202](#)
 - ▼ software security mechanisms to protect information (malicious logic protection)
 - [HSCJ 202,MISM 661](#)
 - ▼ software security mechanisms to protect information (need-to-know controls)
 - [HSCJ 202,MISM 661](#)
 - ▼ software security mechanisms to protect information (operating systems security features)
 - [HSCJ 202](#)
 - ▼ software security mechanisms to protect information (segregation of duties)

HSCJ 202,MISM 661

- ▼* assurance

HSCJ 202

▼ **(d) Network Security**

- ▼ end-to-end access control

HSCJ 202,MISM 670

- ▼ privileges (class, nodes)

HSCJ 202,MISM 670

- ▼ public vs private

HSCJ 202,MISM 670

- ▼ traffic analysis

HSCJ 202,MISM 670

- ▼* dial-up vs dedicated

HSCJ 202,MISM 670

▼ **(e) Administrative Security Procedural Controls**

- ▼ construction, changing, issuing and deleting passwords

HSCJ 202,MISM 661

- ▼ copyright protection and licensing

HSCJ 202,HSCJ 317,MISM 661

- ▼ destruction of media

HSCJ 202,MISM 661

- ▼ documentation, logs and journals

HSCJ 202,MISM 661

- ▼ emergency destruction

HSCJ 202,MISM 661

- ▼ external marking of media

HSCJ 202,MISM 661

- ▼ media downgrade and declassification

HSCJ 202

- ▼ preparation of security plans

HSCJ 202,MISM 661

- ▼ reporting of computer misuse or abuse

HSCJ 202,MISM 661

- ▼ repudiation

HSCJ 202,MISM 661

- ▼ sanitization of media

HSCJ 202,MISM 661

- ▼ transportation of media

HSCJ 202,HSCJ 210,MISM 661

- ▼* attribution

HSCJ 202,MISM 661

▼ **(f) Auditing and Monitoring**

- ▼ effectiveness of security programs

HSCJ 202,MISM 661

- ▼ investigation of security breaches
 - HSCJ 202,HSCJ 210,ISIN 200,MISM 661,MISM 662
- ▼ monitoring systems for accuracy and abnormalities
 - HSCJ 202,MISM 661
- ▼ privacy
 - HSCJ 202,MISM 661
- ▼ review of accountability controls
 - HSCJ 202,MISM 661
- ▼ review of audit trails and logs
 - HSCJ 202,HSCJ 210,MISM 661
- ▼ review of software design standards
 - HSCJ 202,MISM 661
- ▼ verification, validation, testing, and evaluation processes
 - HSCJ 202,MISM 661
- ▼* conducting security reviews
 - HSCJ 202,MISM 661
- ▼ **(g) Cryptosecurity**
 - ▼ electronic key management system
 - HSCJ 202,HSCJ 210,MISM 661
 - ▼ encryption/decryption method, procedure, algorithm
 - HSCJ 202,HSCJ 210,MISM 661
 - ▼* cryptovvariable or key
 - HSCJ 202,HSCJ 315,MISM 661
- ▼ **(h) Key Management**
 - ▼ destruction procedures for COMSEC material
 - HSCJ 202,MISM 661
 - ▼ identify and inventory COMSEC material
 - HSCJ 202,MISM 661
 - ▼ key management protocols (bundling, electronic key, over-the-air rekeying)
 - HSCJ 202,MISM 661
 - ▼ report COMSEC incidents
 - HSCJ 202,HSCJ 210,MISM 661
 - ▼* access, control and storage of COMSEC material
 - HSCJ 202,MISM 661
- ▼ **(i) Transmission Security**
 - ▼ covert channel control (crosstalk)
 - HSCJ 202,MISM 670
 - ▼ dial back
 - HSCJ 202,MISM 670
 - ▼ directional signals
 - HSCJ 202,ISYS 325,MISM 670
 - ▼ frequency hopping
 - HSCJ 202,ISYS 325,MISM 670
 - ▼ jamming

- [HSCJ 202,MISM 670](#)
 - ▼ line-of-sight
 - [HSCJ 202,ISYS 325,MISM 670](#)
 - ▼ line authentication
 - [HSCJ 202,MISM 670](#)
 - ▼ low power
 - [HSCJ 202,MISM 670](#)
 - ▼ masking
 - [HSCJ 202,MISM 670](#)
 - ▼ optical systems
 - [HSCJ 202,ISYS 325,MISM 670](#)
 - ▼ protected wireline
 - [HSCJ 202,MISM 670](#)
 - ▼ screening
 - [HSCJ 202,MISM 670](#)
 - ▼ spread spectrum transmission
 - [HSCJ 202,ISYS 325,MISM 670](#)
 - ▼ * burst transmission
 - [HSCJ 202,ISYS 325,MISM 670](#)
- ▼ **(j) TEMPEST Security**
 - ▼ banding
 - [HSCJ 202,MISM 661](#)
 - ▼ cabling
 - [HSCJ 202,MISM 661](#)
 - ▼ filtered power
 - [HSCJ 202,MISM 661](#)
 - ▼ grounding
 - [HSCJ 202,MISM 661](#)
 - ▼ shielding
 - [HSCJ 202,MISM 661](#)
 - ▼ TEMPEST separation
 - [HSCJ 202,MISM 661](#)
 - ▼ zone of control/zoning
 - [HSCJ 202,MISM 661](#)
 - ▼ * attenuation
 - [HSCJ 202,MISM 661](#)

b. Standard Specifications

**NSTISSI No. 4011
20 June 1994**

NSTISS

**NATIONAL
SECURITY
TELECOMMUNICATIONS
AND
INFORMATION
SYSTEMS
SECURITY**

**NATIONAL TRAINING STANDARD
FOR INFORMATION SYSTEMS
SECURITY (INFOSEC)
PROFESSIONALS**

NSTISS

NATIONAL SECURITY
TELECOMMUNICATIONS
AND INFORMATION
SYSTEMS SECURITY

NATIONAL MANAGER

FOREWORD

1. This instruction provides the minimum course content for the training of information systems security (INFOSEC) professionals in the disciplines of telecommunications security and automated information systems (AIS) security.

2. Representatives of the National Security Telecommunications and Information Systems Security Committee may obtain additional copies of this instruction from:

Executive Secretariat
National Security Telecommunications and
Information Systems Security Committee
National Security Agency
Fort George G. Meade, MD 20755-6000

3. U.S. Government contractors are to contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.

J. M. McCONNELL
Vice Admiral, U.S. Navy

**NATIONAL TRAINING STANDARD
FOR
INFORMATION SYSTEMS SECURITY (INFOSEC) PROFESSIONALS**

	<u>SECTION</u>
PURPOSE	I
SCOPE AND APPLICABILITY	II
REFERENCES.	III
RESPONSIBILITIES.	IV
TRAINING STANDARD	V

SECTION I - PURPOSE

1. This instruction establishes the minimum training standard for the training of information systems security (INFOSEC) professionals in the disciplines of telecommunications and automated information systems (AIS) security.

SECTION II - SCOPE AND APPLICABILITY

2. National Security Telecommunications and Information Systems Security Directive No. 501 establishes the requirement for federal departments and agencies to implement training programs for INFOSEC professionals. As defined in NSTISSD 501, an INFOSEC professional is an individual who is responsible for the security oversight or management of national security systems during phases of the life cycle. That directive is being implemented in a synergistic environment among departments and agencies which are committed to satisfying these INFOSEC education and training requirements in the most effective and efficient manner possible. This instruction is the first in a series of minimum training and education standards which are being developed to assist departments and agencies in meeting their responsibilities in these areas.

3. The body of knowledge listed in this instruction may be obtained from a variety of sources, i.e., the National Cryptologic School, contractors, adaptations of existing department/agency training programs, or a combination of experience and formal training.

4. This instruction is applicable to all departments and agencies of the U.S. Government, their employees, and contractors who are responsible for the security oversight or management of national security systems during each phase of the life cycle.

SECTION III - REFERENCES

5. P.L. 100-235, Computer Security Act of 1987, dated January 8, 1988.

6. National Policy for the Security of National Security Telecommunications and Information Systems, dated July 5, 1990.

7. NSTISSD 501, National Training Program for Information Systems Security (INFOSEC) Professionals, dated 16 November 1992.

8. OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems, December 12, 1985.

9. Office of Personnel Management, 5 CFR Part 930, Training Requirements for the Computer Security Act, January 3, 1992.

10. NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, June 5, 1992.

SECTION IV - RESPONSIBILITIES

11. Heads of U.S. Government departments and agencies will:

a. Ensure that INFOSEC professionals obtain the body of knowledge as outlined in this instruction.

b. Ensure that an INFOSEC training program is an integral part of the overall training program.

c. Require contractors to comply with the provisions of this instruction when they are responsible for the security oversight or management of national security systems operated by or on behalf of the U.S. Government.

12. The National Manager will:

a. Provide and maintain an INFOSEC training standard to U.S. Government departments and agencies.

b. Ensure that appropriate INFOSEC training courses are developed.

c. Assist other U.S. Government departments and agencies in developing and/or conducting INFOSEC training activities as requested.

SECTION V - TRAINING STANDARD

13. Using a comprehensive model of information systems security, the curriculum is intended to provide two levels of knowledge:

a. Awareness Level. Creates a sensitivity to the threats and vulnerabilities of national security information systems, and a recognition of the need to protect data, information and the means of processing them; and builds a working knowledge of principles and practices in INFOSEC.

b. Performance Level. Provides the employee with the skill or ability to design, execute, or evaluate agency INFOSEC security procedures and practices. This level of understanding will ensure that employees are able to apply security concepts while performing their tasks.

14. The program of instruction, as outlined below, shall encompass scope, suggested sequence, and content.

a. COMMUNICATIONS BASICS (Awareness Level)

Instructional Content

Behavioral Outcomes

- | | |
|---|---|
| - Introduce the evolution of modern communications systems. | - Outline chronology of communications systems and development. |
|---|---|

- Describe vehicles of transmission.
- Match features of transmission to descriptors (e.g., signal type, speed production characteristics, etc.)

(1) Topical Content

(a) Historical vs Current Methodology

(b) Capabilities and limitations of various communications systems

- microwave
- line of sight
- satellite
- radio frequency (e.g., bandwidth)
- asynchronous vs synchronous
- dedicated line
- digital vs analog
- public switched network

(1) Topical Content

(a) Historical vs Current Methodology

b. AUTOMATED INFORMATION SYSTEMS (AIS) BASICS (Awareness Level)

Instructional Content

Behavioral Outcomes

- | | |
|--|--|
| - Provide language of an AIS. | - Define terms in an AIS. |
| - Describe an AIS environment by an AIS. | - Define functions performed. |
| - Providing an overview of hardware, software, firmware components of an AIS, to integrate into information systems security aspects/ behaviors discussed later. | - Describe interrelationship among AIS components. |

(1) Topical Content

- (a) Historical vs Current Technology
- (b) Hardware
 - distributed vs stand-alone
 - micro, mini, mainframe processors
 - storage devices
 - components (e.g., input, output, central processing unit (CPU))
- (c) Software
 - operating system
 - applications
- (d) Memory
 - sequential
 - random
 - volatile vs nonvolatile
- (e) Media
 - magnetic remanence
 - optical remanence
- (f) Networks
 - topology
 - sharing of data
 - sharing of devices
 - file servers
 - modems
 - asynchronous vs synchronous
 - switching

c. SECURITY BASICS (Awareness Level)

Instructional Content

- Using the Comprehensive Model of Information Systems Security (contained in the Annex to this instruction), introduce a comprehensive model of information systems security that addresses:
 - critical characteristics of information

Behavioral Outcomes

- The student will list and describe the elements of AIS security.
- The student will summarize security disciplines used in protecting government automated information systems.

- information states, and
- security measures.
- Student will give examples of determinants of critical information.

(1) Topical Content

(a) INFOSEC Overview

- threats
- vulnerabilities
- critical information characteristics
 - confidentiality
 - integrity
 - availability
- information states
 - transmission
 - storage
 - processing
- security countermeasures
 - technology
 - policy, procedures and practices
 - education, training and awareness

(b) Operations Security (OPSEC)

- OPSEC process
- INFOSEC and OPSEC interdependency
- unclassified indicators
- OPSEC surveys/OPSEC planning

(c) Information Security

- policy
- roles and responsibilities
- application dependent guidance

(d) INFOSEC

- cryptography
 - strength (e.g., complexity, secrecy, characteristics of the key)
 - encryption (e.g., point-to-point, network, link)
 - key management (to include electronic key)
- transmission security
- emanations security

- physical, personnel and administrative security
- computer security
 - identification and authentication
 - access control
 - audit
 - object reuse

d. NSTISS BASICS (Awareness Level)

<u>Instructional Content</u>	<u>Behavioral Outcomes</u>
- Describe components (with examples to include: national policy, threats and vulnerabilities, countermeasures, risk management, systems lifecycle management, trust, modes of operation, roles of organizational units, facets of NSTISS.	- Outline national NSTISS Policies. - Cite examples of threats and vulnerabilities of an AIS. - Give examples of Agency implementation of NSTISS policy, practices and procedures.

(1) Topical Content

(a) National Policy and Guidance

- AIS security
- communications security
- protection of information
- employee accountability for agency information

(b) Threats to and Vulnerabilities of Systems

- definition of terms (e.g., threats, vulnerabilities, risk)
- major categories of threats (e.g., fraud, Hostile Intelligence Service (HOIS), malicious logic, hackers, environmental and technological hazards, disgruntled employees, careless employees, HUMINT, and monitoring)
- threat impact areas

- (c) Legal Elements
 - fraud, waste and abuse
 - criminal prosecution
 - evidence collection and preservation
 - investigative authorities
- (d) Countermeasures
 - cover and deception
 - HUMINT
 - monitoring (e.g., data, line)
 - technical surveillance countermeasures
 - education, training, and awareness
 - assessments (e.g., surveys, inspections)
- (e) Concepts of Risk Management
 - threat and vulnerability assessment
 - cost/benefit analysis of controls
 - implementation of cost-effective controls
 - consequences (e.g., corrective action, risk assessment)
 - monitoring the efficiency and effectiveness of controls (e.g., unauthorized or inadvertent disclosure of information)
- (f) Concepts of System Life Cycle Management
 - requirements definition (e.g., architecture)
 - development
 - demonstration and validation (testing)
 - implementation
 - security (e.g., certification and accreditation)
 - operations and maintenance (e.g., configuration management)
- (g) Concepts of Trust
 - policy
 - mechanism
 - assurance
- (h) Modes of Operation
 - dedicated
 - system-high
 - compartmented/partitioned
 - multilevel

- (i) Roles of Various Organizational Personnel
 - senior management
 - program or functional managers
 - system manager and system staff
 - telecommunications office and staff
 - security office
 - COMSEC custodian
 - INFOSEC Officer
 - information resources management staff
 - audit office
 - OPSEC managers
 - end users

- (j) Facets of NSTISS
 - protection of areas
 - protection of equipment
 - protection of passwords
 - protection of files and data
 - protection against malicious logic
 - backup of data and files
 - protection of magnetic storage media
 - protection of voice communications
 - protection of data communications
 - protection of keying material
 - application of cryptographic systems
 - transmission security countermeasures (e.g., callsigns, frequency, and pattern forewarning protection)
 - reporting security violations

e. SYSTEM OPERATING ENVIRONMENT (Awareness Level)

<u>Instructional Content</u>	<u>Behavioral Outcomes</u>
- Outline Agency specific AIS and telecommunications systems.	- Summarize Agency AIS and telecommunications systems in operation.
- Describe Agency "control points" for purchase and maintenance of Agency AIS and telecommunications systems.	- Give examples of current Agency AIS/telecommunications systems and configurations.

- Review Agency AIS and telecommunications security policies.
- List Agency-level contact points for AIS and telecommunications systems and maintenance.
- Cite appropriate policy and guidance.

(1) Topical Content

(a) AIS

- hardware
- software
- firmware

(b) Telecommunications Systems

- hardware
- software

(c) Agency Specific Security Policies

- guidance
- roles and responsibilities
- points of contact

(d) Agency Specific AIS and Telecommunications Policies

- points of contact
- references

f. NSTISS PLANNING AND MANAGEMENT (Performance Level)

Instructional Content

- Discuss practical performance measures employed in designing security measures and programs.
- Introduce generic security planning guidelines/documents.

Behavioral Outcomes

- Builds a security plan that encompasses NSTISS components in designing protection/security for an instructor-supplied description of an AIS telecommunications system.

(1) Topical Content

(a) Security Planning

- directives and procedures for NSTISS policy
- NSTISS program budget
- NSTISS program evaluation
- NSTISS training (content and audience definition)

(b) Risk Management

- information identification
- roles and responsibilities of all the players in the risk analysis process
- risk analysis and/or vulnerability assessment components
- risk analysis results evaluation
- corrective actions
- acceptance of risk (accreditation)

(c) Systems Life Cycle Management

- management control process (ensure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications and into significant modifications to existing applications)
- evaluation of sensitivity of the application based upon risk analysis
- determination of security specifications
- design review and systems test performance (ensure required safeguards are operationally adequate)
- systems certification and accreditation process
- acquisition

(d) Contingency Planning/Disaster Recovery

- contingency plan components
- agency response procedures and continuity of operations

- team member responsibilities in responding to an emergency situation
- guidelines for determining critical and essential workload
- determination of backup requirements
- development of procedures for off-site processing
- development of plans for recovery actions after a disruptive event
- emergency destruction procedures

g. NSTISS POLICIES AND PROCEDURES (Performance Level)

Instructional Content

Behavioral Outcomes

- | | |
|---|--|
| <ul style="list-style-type: none">- List and describe: specific technological, policy, and educational solutions for NSTISS.- List and describe: elements of vulnerability and threat that exist in an AIS/telecommunications system with corresponding protection measures. | <ul style="list-style-type: none">- Playing the role of either a system penetrator or system protector, the student will discover points of exploitation and apply appropriate countermeasures in an instructor-supplied description of an Agency AIS/telecommunications system. |
|---|--|

(1) Topical Content

(a) Physical Security Measures

- building construction
- alarms
- information systems centers
- communications centers
- shielding
- cabling
- filtered power
- physical access control systems (key cards, locks and alarms)
- stand-alone systems and peripherals
- environmental controls (humidity and air conditioning)
- fire safety controls
- storage area controls
- power controls (regulator, uninterrupted power service (UPS), and emergency poweroff switch)
- protected distributed systems

- (b) Personnel Security Practices and Procedures
 - position sensitivity
 - employee clearances
 - access authorization/verification (need-to-know)
 - security training and awareness (initial and refresher)
 - systems maintenance personnel
 - contractors

- (c) Software Security
 - configuration management
 - programming standards and controls
 - documentation
 - change controls
 - software security mechanisms to protect information
 - segregation of duties
 - concept of least privilege
 - identification and authentication
 - access privileges
 - internal labeling
 - application security features
 - audit trails and logging
 - operating systems security features
 - need-to-know controls
 - malicious logic protection
 - assurance

- (d) Network Security
 - public vs private
 - dial-up vs dedicated
 - privileges (class, nodes)
 - traffic analysis
 - end-to-end access control

- (e) Administrative Security Procedural Controls
 - external marking of media
 - destruction of media
 - sanitization of media
 - construction, changing, issuing and deleting passwords
 - transportation of media
 - reporting of computer misuse or abuse
 - preparation of security plans
 - emergency destruction
 - media downgrade and declassification
 - copyright protection and licensing
 - documentation, logs and journals
 - attribution
 - repudiation

- (f) Auditing and Monitoring
 - effectiveness of security programs
 - conducting security reviews
 - verification, validation, testing, and evaluation processes
 - monitoring systems for accuracy and abnormalities
 - investigation of security breaches
 - review of audit trails and logs
 - review of software design standards
 - review of accountability controls
 - privacy

- (g) Cryptosecurity
 - encryption/decryption method, procedure, algorithm
 - cryptovvariable or key
 - electronic key management system

- (h) Key Management
 - identify and inventory COMSEC material
 - access, control and storage of COMSEC material
 - report COMSEC incidents
 - destruction procedures for COMSEC material
 - key management protocols (bundling, electronic key, over-the-air rekeying)

- (i) Transmission Security
 - frequency hopping
 - masking
 - directional signals
 - burst transmission
 - optical systems
 - spread spectrum transmission
 - covert channel control (crosstalk)
 - dial back
 - line authentication
 - line-of-sight
 - low power
 - screening
 - jamming
 - protected wireline

- (j) TEMPEST Security
 - shielding
 - grounding
 - attenuation
 - banding
 - filtered power
 - cabling
 - zone of control/zoning
 - TEMPEST separation

Enclosure:

Information Systems Security: A Comprehensive Model

ANNEX

INFORMATION SYSTEMS SECURITY: A COMPREHENSIVE MODEL ¹

INTRODUCTION

This Annex serves as a comprehensive model for the security of information systems and also functions as an assessment, systems development, and evaluation tool. The model is unique in that it stands independent of technology. Its application is universal and is not constrained by organizational differences. As with all well-defined fundamental concepts, it is unnecessary to alter the premise even as technology and human understanding evolve.

Computers communicate. Communications systems compute. The evolution of technology has long since eliminated any arbitrary distinction between a computer and its communication components or a communications network and its computing system. Some organizations have attempted to deal with the phenomenon by marrying these functions under common leadership. This has resulted in hyphenated job descriptions such as Computer-Communications Systems Staff Officer and names like Information Technology Group. Unfortunately, these names can mask an inappropriate or poorly executed realignment of organizational responsibilities. Ideally, management will recognize there is a theoretical as well as organizational impact.

The same is true for the security disciplines. Merely combining the communications security (COMSEC) and computer security (COMPUSEC) disciplines under an umbrella of common management is unacceptable. Even if we address the other, albeit less technical, aspects of information systems security such as policy, administration, and personnel security, we still fail to develop a comprehensive view of this evolving technology. The reason for this becomes clear when we are reminded it's the information that is the cornerstone of information systems security. In this sense, any paradigm which emphasizes the technology at the expense of information will be lacking.

1. Capt John R. McCumber, Joint Staff, as extracted from the proceedings of the 14th National Computer Security Conference, October 1991.

THE NATURE OF INFORMATION

Defining the nature of information could be a tedious task. To some it represents the free flowing evolution of knowledge; to others, it is intelligence to be guarded. Add to this the innumerable media through which the information is perceived and we have a confusing array of contradictions. How can we present a study of information that has universal application?

It may be best to develop a simple analogy. The chemical compound H^2O means many things to all of us. In its liquid state, water means life-giving sustenance to a desert-dwelling Bedouin; to a drowning victim, it is the vehicle of death. The same steam we use to prepare vegetables could scald an unwary cook. Ice can impede river-borne commerce on the Mississippi River or make a drink more palatable. Science, therefore, does not deal with the perception of the compound, but with its state.

As the compound H^2O can be water, ice or steam, information has three basic states. At any given moment, information is being transmitted, stored, or processed. The three states exist irrespective of the media in which information resides. This subtle distinction ultimately allows us to encompass all information systems technology in our model.

It is possible to look at the three states in microcosm and say that processing is simply specialized state combinations of storage and transfer; so, in fact, there are only two possible states. By delving to this level of abstraction, however, we go beyond the scope and purpose of the model. The distinction between the three states is fundamental and necessary to accurately apply the model. For example, cryptography can be used to protect information while it's transferred through a computer network and even while it is stored in magnetic media. However, the information must be available in plaintext (at least to the processor) in order for the computer to perform the processing function. The processing function is a fundamental state that requires specific security controls.

When this information is needed to make a decision, the end user may not be aware of the number of state changes effected. The primary concern will be certain characteristics of the information. These characteristics are intrinsic and define the security-relevant qualities of the information. As such, they are the next major building block of our information systems security model.

CRITICAL INFORMATION CHARACTERISTICS

Information systems security concerns itself with the maintenance of three critical characteristics of information: confidentiality (Pfleeger's "secrecy"), integrity, and availability [PFL89]. These attributes of information represent the full spectrum of security concerns in an automated environment. They are applicable for any organization irrespective of its philosophical outlook on sharing information.

CONFIDENTIALITY

Confidentiality is the heart of any security policy for an information system. A security policy is the set of rules that, given identified subjects and objects, determines whether a given subject can gain access to a specific object [DOD85]. In the case of discretionary access controls, selected users (or groups) are controlled as to which data they may access. Confidentiality is then the assurance that access controls are enforced. Confidentiality is used instead of secrecy to avoid unwarranted implications that this is solely the domain of governments.

All organizations have a requirement to protect certain information. Even owners of a clearinghouse operation or electronic bulletin need the ability to prevent unwanted access to supervisory functions within their system. It's also important to note the definition of data, which must be protected with confidentiality controls, is broadening throughout government [OTA87]. Actual information labeling and need-to-know imperatives are aspects of the system security policy that are enforced to meet confidentiality objectives. The issue of military versus civilian security controls is one which need not impact the development of a comprehensive representation of information systems security principles.

INTEGRITY

Integrity is perhaps the most complex and misunderstood characteristic of information. We seem to have a better foundation in the development of confidentiality controls than those which can help ensure data integrity. Pfleeger defines integrity as "assets" (which) can only be modified by authorized parties" [PFL89]. Such a definition unnecessarily confines the concept to one of access control.

A much broader definition is used here. Data integrity is a matter of degree (as is the concept of "trust" as applied to trusted systems) that has to be defined as a quality of the information and not as who does/does not have access to it. Integrity is that quality of information that identifies how closely the data represent reality. How closely does your resume reflect "you?" Does the credit report accurately reflect the individual's historical record of financial transactions? The definition of integrity must include the broad scope of accuracy, relevancy, and completeness.

Data integrity calls for a comprehensive set of aids to promote accuracy and completeness as well as security. This is not to say that too much information can't be a problem. Data redundancy and unnecessary records present a variety of challenges to system implementors and administrators. The users must define their needs in terms of the information necessary to perform certain functions. Information systems security functions help ensure this information is robust and (to the degree necessary) reflects the reality it is meant to represent.

AVAILABILITY

Availability is a coequal characteristic with confidentiality and integrity. This vital aspect of security ensures the information is provided to authorized users when it's requested or needed. Often it's viewed as a less technical requirement that is satisfied by redundancies within the information system such as back-up power, spare data channels, and parallel data bases. This perception, however, ignores one of the most valuable aspects of our model that this characteristic provides. Availability is the check-and-balance constraint on our model. Because security and utility often conflict, the science of information systems security is also a study of subtle compromises.

As well as ensuring system reliability, availability acts as a metric for determining the extent of information systems security breaches [DOJ88]. Ultimately, when information systems security preventive measures fail, remedial action may be necessary. This remedial activity normally involves support from law enforcement or legal departments. In order to pursue formal action against people who abuse information systems resources, the ability to prove an adverse impact often hinges

on the issue of denying someone the availability of information resources. Although violations of information confidentiality and integrity can be potentially more disastrous, denial of service criteria tend to be easier to quantify and thus create a tangible foundation for taking action against violators [CHR90].

The triad of critical information characteristics covers all aspects of security-relevant activity within the information system. By building a matrix with the information states (transmission, storage, processing) positioned along the horizontal axis and the critical information (confidentiality, integrity, availability) characteristics aligned down the vertical, we have the foundation for the model.

SECURITY MEASURES

We've now outlined a matrix that provides us with the theoretical basis for our model. What it lacks at this stage is a view of the measures we employ to ensure the critical information characteristics are maintained while information resides in or moves between states. It's possible, at this point, to perceive the chart as a checklist. At a very high level of abstraction, one could assess the security posture of a system by using this approach. For example, you may single out systems information confidentiality during transmission or any intersection area for scrutiny.

The two-dimensional matrix also has another less obvious utility. We can map various security technologies into the nine boxes. Using our example from above, we note it is necessary to protect the confidentiality of the information during its transmission state. We can then determine which security technologies help ensure confidentiality during transmission of the information. In this case, cryptography would be considered a primary security technology. We can then place various cryptographic techniques and products within a subset in this category. Then we repeat the process with other major types of technology that can be placed within these spaces. The procedure is repeated for all nine blocks on our grid. Thus we form the first of three layers which will become the third dimension of our model--security measures.

TECHNOLOGY

The technology layer will be the primary focus of the third dimension. We will see that it provides the basis for the other two layers. For our purposes, we can define technology as any physical device or technique implemented in physical form that is specifically used to help ensure the critical information characteristics are maintained through any of the information states. Technology can be implemented in hardware, firmware, or software. It could be a biometric device, cryptographic module, or security-enhanced operating system. When we think of a thing, which could be used to protect the critical characteristics of information, we are thinking of technology.

Usually organizations are built around functional responsibilities. The advent of computer technology created the perception that a group needed to be established to accommodate the new machines that would process, store, and transmit much of our vital information. In other words, the organization was adapted to suit the evolving technology. Is this wrong? Not necessarily; however, it is possible to create the impression that technology exists for technology's sake. Telecommunications and computer systems are simply media for information. The media need to be adapted to preserve certain critical characteristics with the adaptation and use of the information media (technology). Adaptation is a design problem, but use and application concerns bring us to the next layer.

POLICY AND PRACTICE

The second layer of the third dimension is that of policy and practice. It's the recognition of the fact that information systems security is not just a product that will be available at some future date. Because of our technology focus, it's easy to begin to think of security solutions as devices or add-on packages for existing information systems. We are guilty of waiting for technology to solve that which is not solely a technological problem. Having an enforceable (and enforced) policy can aid immeasurably in protecting information.

A study has shown 75% of federal agencies don't have a policy for the protection of information on PC-based information systems [OTA87]. Why, if it is so effective, is policy such a neglected security measure? It may be due in part to the evolving social and moral ethic with regard to our use of

information systems. The proliferation of unauthorized software duplication is just another symptom of this problem. Even though software companies have policies and licensing caveats on their products, sanctions and remedies allowed by law are difficult if not impossible to enforce. No major lawsuit involving an individual violator has come before our courts, and it appears many people don't see the harm or loss involved. Although there are limits established by law, it seems we as "society" accept a less stringent standard.

Closely associated with the matter of policy is that of practice. A practice is a procedure we employ to enhance our security posture. For example, we may have a policy that states that passwords must be kept confidential and may only be used by the uniquely-authenticated user. A practice, which helps ensure this policy is followed, would be committing the password to memory rather than writing it somewhere.

The first two layers of the third dimension represent the design and application of a security-enhanced information system. The last building block of our model represents the understanding necessary to protect information. Although an integral aspect of the preceding two layers, it must be considered individually as it is capable of standing alone as a significant security measure.

EDUCATION, TRAINING, AND AWARENESS

The final layer of our third dimension is that of education, training, and awareness. As you will see, were the model laid on its back like a box, the whole model would rest on this layer. This phenomenon is intentional. Education, training, and awareness may be our most prominent security measures, for only by understanding the threats and vulnerabilities associated with our proliferating use of automated information systems can we begin to attempt to deal effectively with other control measures.

Technology and policy must rely heavily on education, training, and awareness from numerous perspectives. Our upcoming engineers and scientists must understand the principles of information security if we expect them to consider the protection of information in the systems they design. Currently, nearly all university graduates in computer science have no formal introduction to information security as part of their education [HIG89].

Those who are responsible for promulgating policy and regulatory guidance must place bounds on the dissemination of information. They must ensure information resources are distributed selectively and securely. The issue is ultimately one of awareness. Ultimate responsibility for its protection rests with those individuals and groups that create and use this information; those who use it to make critical decisions must rely on its confidentiality, integrity, and availability. Education, training and awareness promises to be the most effective security measure in the near term.

Which information requires protection is often debated in government circles. One historic problem is the clash of society's right to know and an individual's right to privacy. It's important to realize that these are not bipolar concepts. There is a long continuum that runs between the beliefs that information is a free flowing exchange of knowledge and that it is intelligence that must be kept secret. From a governmental or business perspective, it must be assumed that all information is intelligence. The question is not should information be protected, but how do we intend to protect the confidentiality, integrity, and availability of it within legal and moral constraints?

THE MODEL

OVERVIEW

The completed model is depicted below. There are nine distinct boxes, each three layers deep. All aspects of information systems security can be viewed within the framework of the model. For example, we may cite a cryptographic module as technology that protects information in its transmission state. What many information system developers fail to appreciate is that for every technology control there is a policy (sometimes referred to as doctrine) that dictates the constraints on the application of that technology. It may also specify parameters that delimit the control's use and may even cite degrees of effectiveness for different applications. Doctrine (policy) is an integral yet distinct aspect of the technology. The third layer--education, training, and awareness then functions as a catalyst for proper application and use of the technology based on the policy (practice) application.

Not every security measure begins with a specific technology. A simple policy or practice often goes a long way in the protection of information assets. This policy or practice is then effected by communicating it to employees through the education, training and awareness level alone. This last layer is ultimately involved in all aspects of the information systems security model. The model helps us understand the comprehensive nature of information security.

CHART GOES HERE
Call Secretariat for copy of drawing

USE OF THE MODEL

The model has several significant applications. Initially, the two-dimensional matrix is used to identify information states and system vulnerabilities. Then, the three layers of security measures can be employed to minimize these vulnerabilities based on a knowledge of the threat to the information asset. Let's take a brief look at these applications.

A developer would begin using the model by defining the various information states within the system. When an information state is identified, one then works down the vertical path to address all three critical information characteristics identifying the vulnerabilities. Once vulnerabilities are noted in this fashion, it becomes a simple matter of working down through the three layers of security measures. If a specific technology is available, the designer knows that policy and practice, as well as education, training, and awareness will be logical follow-on aspects of that control. If a technology cannot be identified, then policy/practice must be viewed as the next likely avenue. If none of the first two layers can satisfactorily counter the vulnerability then, as a minimum, an awareness of the weakness becomes important and fulfills the dictates of the model at the third layer.

Another important application is realized when the model is used as an evaluation tool. As in the design and development application, the evaluator first identifies the different information states within the system. These states can be identified separately from a specific technology. A valuable aspect of the model is the designer need not consider the medium.

After identifying all the states, an evaluator or auditor can perform a comprehensive review much the same way the systems designer used the model during the development phase. For each vulnerability discovered, the same model is used to determine appropriate security measures. It is important to note that a vulnerability may be left unsecured (at an awareness level in the third layer) if the designer or evaluator determines no threat to that vulnerability exists. Although no security practitioner should be satisfied with glaring vulnerabilities, a careful study of potential threats to the information may disclose that the cost of the security measure is more than the loss should the vulnerability be exploited. This is one of the subtle compromises alluded to earlier.

The model can also be used to develop comprehensive information systems security policy and guidance necessary for any organization. With an accurate understanding of the relation of policy to technology and education, training, and awareness, you can ensure your regulations address the entire spectrum of information security. It's of particular importance that corporate and government regulations not be bound by technology. Use of this model allows management to structure its policy outside the technology arena.

The model functions well in determining requirements for education, training, and awareness. Since this is the last layer, it plays a vital role in the application of all the security measures. Even if a designer, evaluator, or user determines to ignore a vulnerability (perhaps because of a lack of threat), then the simple acknowledgement of this vulnerability resides in the last layer as "awareness." Ultimately, all technology, policies, and practices must be translated to the appropriate audience through education, training, and awareness. This translation is the vehicle that makes all security measures effective. For a more complete understanding of the nuances of education, training, and awareness see [MAC89].

The 27 individual "cubes" created by the model can be extracted and examined individually. This key aspect can be useful in categorizing and analyzing countermeasures. It's also a tool for defining organizational responsibility for information security. By considering all 27 such "cubes", the analyst is assured of a complete perspective of all available security measures. This model connotes a true "systems" viewpoint.

CONCLUSION

The information systems security model acknowledges information, not technology, as the basis for our security efforts. The actual medium is transparent in the model. This eliminates unnecessary distinctions between Communications Security (COMSEC), Computer Security (COMPUSEC), Technical Security (TECHSEC), and other technology-defined security sciences. As a result, we can model the security relevant processes of information throughout an entire information system-automated or not.






This model responds to the need for a theoretical foundation for modeling the information systems security sciences. The process begins now by acknowledging the central element in all our efforts--information. Only when we build on this foundation will we accurately address the needs of information systems security in the next decade and beyond.

REFERENCES

- [CHR90] Interview with Agent Jim Christy, Chief, Air Force Office of Special Investigations, Computer Crime Division, 26 March 1990.
- [DOD85] Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, Department of Defense, Washington, DC, December 1985.
- [DOJ88] Basic Considerations in Investigating and Proving Computer-Related Federal Crimes, U.S. Department of Justice, Justice Management Division, Washington, DC, November 1988.
- [HIG89] Higgins, John C., Information Security as a Topic in Undergraduate Education of Computer Scientists, Proceedings of the 12th National Computer Security Conference, November 1989.
- [MAC89] Maconachy, W.V., Computer Security Education, Training, and Awareness: Turning a Philosophical Orientation into Practical Reality, Proceedings of the 12th National Computer Security Conference, November 1989.
- [OTA87] U.S. Congress, Office of Technology Assessment, Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information, OTA-CIT-310, Washington, DC, U.S. Government Printing Office, October 1987.
- [PFL89] Pfleeger, Charles P., Security in Computing, Prentice-Hall, 1989.

C. CNSS Standard NTSTISSI 4012

a. Course Mapping Details

 Print	 Collapse All	 Expand All	 Previous Page	 Next Page
---	--	--	---	--

Welcome Barbara Ciaramitaro, it is Monday, August 16, 2010 at 03:34:17 PM
You are currently viewing a report for CNSI 4012 sorted by element.

▼ **FUNCTION 1 - GRANT FINAL ATO**

▼ **A. Responsibilities**

▼ **1. Aspects of Security**

- ▼ *Explain the importance of SSM role in Information Assurance (IA)

[HSCJ 202](#)

[MISM 661](#)

▼ **2. Accreditation**

- ▼ Discuss the certification process leading to successful accreditation

[HSCJ 202](#)

[MISM 661](#)

- ▼ Discuss the significance of NSTISSP No. 6

[HSCJ 202](#)

[MISM 661](#)

- ▼ Explain the importance of accreditation

[HSCJ 202](#)

[MISM 661](#)

- ▼ Explain types of accreditation

[HSCJ 202](#)

[MISM 661](#)

- ▼ Facilitate the certification process leading to successful accreditation

[HSCJ 202](#)

[MISM 661](#)

- ▼ *Discuss accreditation

[HSCJ 202](#)

[MISM 661](#)

▼ **B. Approvals**

▼ **1. Approval to Operate (ATO)**

- ▼ Discuss purpose and contents of ATO

[HSCJ 202](#)

[MISM 661](#)

- ▼ Explain the importance of risk assessment to support granting an ATO

[HSCJ 202](#)

[MISM 661](#)

- ▼ *Explain ATO

[HSCJ 202](#)

[MISM 661](#)

▼ **2. Interim Approval to Operate (IATO)**

- ▼ Explain the importance of risk assessment to support granting an IATO

[HSCJ 202](#)

[MISM 661](#)

- ▼ Explain the purpose and contents of IATO

HSCJ 202

MISM 661

- ▼ Facilitate implementation of risk mitigation strategies necessary to obtain IATO

HSCJ 202

MISM 661

- ▼*Describe IATO

HSCJ 202

MISM 661

▼ **3. Recertification**

- ▼ Direct the recertification effort

HSCJ 202

MISM 661

- ▼ Explain the importance of the recertification process

HSCJ 202

MISM 661

- ▼ Identify characteristics of information systems that need re-certification

HSCJ 202

MISM 661

- ▼ Initiate the recertification effort

HSCJ 202

MISM 661

- ▼*Describe recertification

HSCJ 202

MISM 661

▼ **4. Systems Security Authorization Agreement (SSAA)**

- ▼ Explain the importance of the SSAA

HSCJ 202

MISM 661

- ▼*Discuss the Systems Security Authorization Agreement (SSAA)

HSCJ 202

MISM 661

▼ **5. Waive Policy to Continue Operation**

- ▼ Discuss risk mitigation strategies necessary to obtain waiver

HSCJ 202

MISM 661

- ▼ Ensure risk assessment supports granting waiver

HSCJ 202

MISM 661

- ▼*Discuss justification for waiver

HSCJ 202

MISM 661

▼ **FUNCTION 2 - REVIEW ACCREDITATION**

▼ **A. Threats**

▼ **1. Attacks**

- ▼ Explain the importance of threats/attacks on systems

HSCJ 202

HSCJ 210

MISM 661

- ▼ *Discuss threats/attacks to systems

HSCJ 202

HSCJ 210

MISM 661

▼ **2. Environmental/Natural Threats**

- ▼ *Discuss environmental/natural threats

HSCJ 202

MISM 661

▼ **3. Human Threats**

- ▼ *Explain the importance of intentional and unintentional human threats

HSCJ 202

MISM 661

▼ **4. Theft**

- ▼ *Explain the importance of theft

HSCJ 202

HSCJ 317

MISM 661

▼ **5. Threat**

- ▼ Explain the importance of organizational threats

HSCJ 202

ISIN 330

MISM 661

- ▼ *Explain threat

HSCJ 202

MISM 661

▼ **6. Threat Analysis**

- ▼ *Explain the importance of threat analysis

HSCJ 202

MISM 661

▼ **7. Threat Assessment**

- ▼ *Explain the importance of threat assessment

HSCJ 202

MISM 661

▼ **B. Countermeasures**

▼ **1. Education, Training, and Awareness as Countermeasures**

- ▼ Ensure educational training, and awareness countermeasures are implemented

HSCJ 202

MISM 661

- ▼ *Explain the importance of educational training, and awareness as countermeasures

HSCJ 202

MISM 661

▼ **2. Procedural Countermeasures**

- ▼ Ensure procedural/administrative countermeasures are implemented

HSCJ 202

MISM 661

- ▼ *Explain the importance of procedural/administrative countermeasures
 - HSCJ 202
 - MISM 661
- ▼ **3. Technical Countermeasures**
 - ▼ Ensure technical/automated countermeasures/deterrents are implemented
 - HSCJ 202
 - MISM 661
 - ▼ Explain the importance of technical countermeasures/deterrents
 - HSCJ 202
 - MISM 661
 - ▼ *Explain the importance of automated countermeasures/deterrents
 - HSCJ 202
 - MISM 661
- ▼ **C. Vulnerability**
 - ▼ **1. Vulnerability**
 - ▼ *Explain vulnerability
 - HSCJ 202
 - MISM 661
 - MISM 662
 - ▼ **2. Vulnerability Analysis**
 - ▼ *Explain the importance of vulnerability analysis
 - HSCJ 202
 - MISM 661
 - MISM 662
 - ▼ **3. Network Vulnerabilities**
 - ▼ *Explain the importance of network vulnerabilities
 - HSCJ 202
 - MISM 661
 - MISM 662
 - ▼ **4. Technical Vulnerabilities**
 - ▼ *Explain the importance of technical vulnerabilities
 - HSCJ 202
 - MISM 661
 - MISM 662
- ▼ **D. Risk Management**
 - ▼ **1. Cost/Benefit Analysis of Information Assurance**
 - ▼ *Explain the importance of cost/benefit analysis of information assurance
 - HSCJ 202
 - MISM 661
 - ▼ **2. Documentation**
 - ▼ *Explain the importance of documentation role in reducing risk
 - HSCJ 202
 - MISM 661
 - ▼ **3. Risk**
 - ▼ Discuss principles of risk
 - HSCJ 202
 - MISM 661

- ▼*Explain risk

HSCJ 202

MISM 661

▼4. Risk Assessment

- ▼*Explain the importance of risk assessment

HSCJ 202

MISM 661

▼5. Risk Management

- ▼*Explain the importance of risk management

HSCJ 202

MISM 661

▼6. Residual Risk

- ▼*Explain residual risk

HSCJ 202

MISM 661

▼7. Risk Acceptance Process

- ▼*Explain the importance of the risk acceptance process

HSCJ 202

MISM 661

▼8. Systems Security Authorization Agreement (SSAA)

- ▼ Discuss the contents of SSAA

HSCJ 202

MISM 661

- ▼ Discuss the purpose of SSAA

HSCJ 202

MISM 661

- ▼ Ensure the certifier understands the mission and it is reflected in SSAA the C&A effort leading to SSAA

HSCJ 202

MISM 661

- ▼ Facilitate effort leading to SSAA

HSCJ 202

MISM 661

- ▼*Explain the importance of the certification and accreditation (C&A) effort leading to accreditation

HSCJ 202

MISM 661

▼ FUNCTION 3 - VERIFY COMPLIANCE

▼ A. Laws Related To Information Assurance (Ia) And Security

▼ 1. Copyright Protection and Licensing

- ▼ Explain the importance of licensing

HSCJ 202

MISM 661

- ▼*Explain the importance of copyright protection

HSCJ 202

MISM 661

▼ 2. Criminal Prosecution

- ▼*Explain the importance of criminal prosecution

HSCJ 202

HSCJ 210

MISM 661

▼3. Due Diligence

- ▼*Explain the importance of due diligence

HSCJ 202

HSCJ 210

MISM 661

▼4. Evidence Collection and Preservation

- ▼Explain the importance of evidence preservation

HSCJ 202

HSCJ 210

MISM 661

- ▼*Explain the importance of evidence collection

HSCJ 202

HSCJ 210

MISM 661

▼5. Fraud, Waste, and Abuse

- ▼*Explain fraud, waste, and abuse

HSCJ 202

HSCJ 317

MISM 661

▼6. Laws Related To Information Assurance and Security

- ▼Discuss implications of Public Law 107-347 regarding certification and accreditation

HSCJ 202

MISM 661

- ▼Explain the importance of implications of Federal Managers Financial Integrity Act of 1982

HSCJ 202

MISM 661

- ▼Explain the importance of implications of Federal Property and Administration Service Act

HSCJ 202

MISM 661

- ▼Explain the importance of implications of legal issues which can affect Information Assurance (IA)

HSCJ 202

HSCJ 317

MISM 661

- ▼Explain the importance of implications of National Archives and Records Act

HSCJ 202

MISM 661

- ▼Explain the importance of implications of the Computer Fraud and Abuse Act, P.L. 99- 474, 18 U.S. Code 1030

HSCJ 202

MISM 661

- ▼Explain the importance of implications of the Freedom of Information Act and Electronic Freedom of Information Act

HSCJ 202
MISM 661

- ▼ Explain the importance of implications of the legal responsibilities of senior systems managers

HSCJ 202
MISM 661

- ▼ Explain the importance of implications of the Privacy Act

HSCJ 202
MISM 661

- ▼ Explain the importance of implications of USA Patriot Act, GPEA, and Paperwork Reduction Acts

HSCJ 202
ISIN 330
MISM 661

- ▼ Explain the importance of Public Law 107-347, E-Government Act Of 2002, Title III, Federal Information Security Management Act (FISMA), 17 Dec 02

HSCJ 202
MISM 661

- ▼*Explain the importance of implications of Electronic Records Management and Federal Records Act

HSCJ 202
MISM 661

▼ **7. Legal and Liability Issues**

- ▼*Explain the importance of legal and liability issues as they apply to system and mission

HSCJ 202
HSCJ 317
MISM 661

▼ **8. Ethics**

- ▼*Discuss ethics

HSCJ 202
MISM 661

▼ **B. Policy Direction**

▼ **1. Access Control Policies**

- ▼*Explain the importance of access control policies

HSCJ 202
MISM 661

▼ **2. Administrative Security Policies And Procedures**

- ▼*Explain the importance of administrative security policies/procedures

HSCJ 202
MISM 661

▼ **3. Audit Trails and Logging Policies**

- ▼ Explain the importance of logging policies

HSCJ 202
MISM 661

- ▼*Explain the importance of audit trail policy

HSCJ 202
MISM 661

▼ **4. Documentation Policies**

- ▼ *Explain the importance of documentation policies

HSCJ 202
MISM 661

▼ **5. Evidence Collection and Preservation Policies**

- ▼ *Explain the importance of evidence collection/preservation policies

HSCJ 202
HSCJ 210

▼ **6. Information Security Policy**

- ▼ Explain the importance of information security policy

HSCJ 202
MISM 661

- ▼ *Define information security policy

HSCJ 202
MISM 661

▼ **7. National Information Assurance (IA) Certification & Accreditation (C&A) Process Policy**

- ▼ *Explain the importance of the National Information Assurance (IA) Certification & Accreditation (C&A) Policy

HSCJ 202
MISM 661

▼ **8. Personnel Security Policies & Guidance**

- ▼ Explain the importance of personnel security guidance

HSCJ 202
MISM 661

▼ **C. Security Requirements**

▼ **1. Access Authorization**

- ▼ *Explain the importance of access authorization

HSCJ 202
MISM 661

▼ **2. Auditable Events**

- ▼ *Explain auditable events

HSCJ 202
MISM 661

▼ **3. Authentication**

- ▼ *Explain authentication

HSCJ 202
MISM 661

▼ **4. Background Investigations**

- ▼ *Explain the importance of background investigations

HSCJ 202
MISM 661

▼ **5. Countermeasures**

- ▼ *Explain the importance of countermeasures

HSCJ 202
MISM 661

▼ **6. Delegation of Authority**

- ▼ Ensure that individuals are assigned to perform IA functions

HSCJ 202

MISM 661

- ▼*Discuss the importance of delegation of authority

HSCJ 202

MISM 661

▼ **7. Education, Training, and Awareness**

- ▼ Ensure educational, training, and awareness countermeasures are implemented

HSCJ 202

MISM 661

- ▼*Explain the importance of education, training, and awareness as countermeasures

HSCJ 202

MISM 661

▼ **8. Electronic Records Management**

- ▼ Explain the importance of electronic records management

HSCJ 202

MISM 661

- ▼*Discuss electronic records management

HSCJ 202

MISM 661

▼ **9. Electronic-Mail Security**

- ▼ Explain the importance of electronic-mail security

HSCJ 202

MISM 661

- ▼*Discuss electronic-mail security

HSCJ 202

MISM 661

▼ **10. Information Classification**

- ▼ Explain the importance of information classification

HSCJ 202

MISM 661

- ▼*Discuss information classification

HSCJ 202

MISM 661

▼ **11. Investigative Authorities**

- ▼ Explain the importance of investigative authorities

HSCJ 202

HSCJ 210

MISM 661

- ▼*Discuss investigative authorities

HSCJ 202

HSCJ 210

MISM 661

▼ **12. Key Management Infrastructure**

- ▼*Discuss key management infrastructure

HSCJ 202

HSCJ 315

MISM 661

▼ **13. Information Marking**

- ▼ *Discuss information marking

HSCJ 202
MISM 661

▼ **14. Non-repudiation**

- ▼ Explain the importance and role of non-repudiation

HSCJ 202
MISM 661

- ▼ *Discuss non-repudiation

HSCJ 202
MISM 661

▼ **15. Public Key Infrastructure (PKI)**

- ▼ Explain the importance and role of PKI

HSCJ 202
HSCJ 315
MISM 661

▼ **FUNCTION 4 - ENSURE ESTABLISHMENT OF SECURITY CONTROLS**

▼ **A. Administration**

▼ **1. Accountability for Classified/Sensitive Data**

- ▼ Discuss classification and declassification of information

HSCJ 202
MISM 661

- ▼ *Explain the importance of accountability for sensitive data

HSCJ 202
MISM 661

▼ **2. Automated Security Tools**

- ▼ *Explain the importance of automated security tools

HSCJ 202
MISM 661

▼ **3. Backups**

- ▼ Explain the importance of backups

HSCJ 202
MISM 661

- ▼ *Discuss backups

HSCJ 202
MISM 661

▼ **4. Change Control/Configuration Management**

- ▼ Discuss configuration management

HSCJ 202
MISM 661

- ▼ Explain the importance of configuration management

HSCJ 202
MISM 661

- ▼ *Discuss change control

HSCJ 202
MISM 661

▼ **5. Declassification/Downgrade of Media**

- ▼ Discuss the importance of downgrade of information

HSCJ 202

MISM 661

- ▼*Explain the importance of downgrade of media

HSCJ 202

MISM 661

- ▼ **6. Destruction/Purging/Sanitization of Classified/Sensitive Information**

- ▼*Explain the importance of destruction/purging/sanitization procedures for classified/sensitive information

HSCJ 202

MISM 661

- ▼ **B. Access**

- ▼ **1. Access Controls**

- ▼ Explain the importance of manual/automated access controls

HSCJ 202

MISM 661

- ▼*Define manual/automated access controls

HSCJ 202

MISM 661

- ▼ **2. Access Privileges**

- ▼*Explain the importance of access privileges

HSCJ 202

MISM 661

- ▼ **3. Discretionary Access Controls**

- ▼ Explain the importance of discretionary access controls

HSCJ 202

MISM 661

- ▼*Discuss discretionary access controls

HSCJ 202

MISM 661

- ▼ **4. Mandatory Access Controls**

- ▼ Explain the importance of mandatory access controls

HSCJ 202

MISM 661

- ▼*Define mandatory access controls

HSCJ 202

MISM 661

- ▼ **5. Biometrics/Biometric Policies**

- ▼*Explain biometric policies

HSCJ 202

MISM 661

- ▼ **6. Separation of Duties**

- ▼ Explain the importance of the need to ensure separation of duties where necessary

HSCJ 202

MISM 661

- ▼*Define the need to ensure separation of duties where necessary

HSCJ 202

MISM 661

▼ **7. Need-To-Know Controls**

- ▼ Explain the importance of need to know controls

HSCJ 202

MISM 661

- ▼ *Define need to know controls

HSCJ 202

MISM 661

▼ **C. Incident Handling And Response**

▼ **1. Emergency Destruction Procedures**

- ▼ *Explain the importance of emergency destruction procedures

HSCJ 202

MISM 661

▼ **2. Organizational/Agency Information Assurance Emergency Response Teams**

- ▼ *Explain the role of organizational/agency information assurance emergency response teams

HSCJ 202

HSCJ 210

MISM 661

▼ **D. Continuity Of Operations Planning**

▼ **1. Business Recovery**

- ▼ Explain the importance of business recovery

HSCJ 202

MISM 661

- ▼ *Define business recovery

HSCJ 202

MISM 661

▼ **2. Contingency/Continuity of Operations Planning**

- ▼ Ensure the establishment and testing of contingency/continuity of operations plans

HSCJ 202

MISM 661

- ▼ *Explain the importance of contingency/continuity of operations planning

HSCJ 202

MISM 661

▼ **3. Disaster Recovery**

- ▼ *Explain the importance of disaster recovery

HSCJ 202

MISM 661

▼ **4. Disaster Recovery Plan**

- ▼ Ensure the establishment and testing of recovery plans

HSCJ 202

MISM 661

- ▼ *Explain the importance of recovery plan

HSCJ 202

MISM 661

▼ **5. Incident response policies**

- ▼*Explain the importance of incident response policy

HSCJ 202
HSCJ 210

- ▼ **6. Law enforcement interfaces/policies**

- ▼Discuss law enforcement policies

HSCJ 202
HSCJ 210
MISM 661

- ▼ Explain the importance of law enforcement interfaces

HSCJ 202
HSCJ 210

- ▼*Discuss law enforcement interfaces

HSCJ 202
HSCJ 210
MISM 661

- ▼ **7. Reconstitution**

- ▼ Explain the importance of principles of system reconstitution

HSCJ 202
MISM 661

- ▼*Define principles of system reconstitution

HSCJ 202
MISM 661

- ▼ **8. Restoration**

- ▼*Explain the importance of restoration to continuity of operation

HSCJ 202
MISM 661

- ▼ **FUNCTION 5 - ENSURE PROGRAM MANAGERS DEFINE SECURITY IN ACQUISITIONS**

- ▼ **A. Acquisition**

- ▼ **1. Certification Test & Evaluation (CT&E)**

- ▼Discuss the importance of CT&E as part of acquisition process

HSCJ 202
MISM 661

- ▼*Define CT&E as part of acquisition process

HSCJ 202
MISM 661

- ▼ **2. Certification Tools**

- ▼*Discuss significance/results of certification tools

HSCJ 202
MISM 661

- ▼ **3. Product Assurance**

- ▼ Explain the importance of protection profiles

HSCJ 202
MISM 661

- ▼ Explain the importance of security targets

HSCJ 202
MISM 661

- ▼*Explain the importance of product assurance role in acquiring systems, i.e., NSTISSP No. 11, Jan 00

HSCJ 202

MISM 661

▼ **4. Contracting For Security Services**

- ▼ Define where contracting for security services is appropriate

HSCJ 202

MISM 661

- ▼ Explain threats from contracting for security services

HSCJ 202

MISM 661

- ▼*Discuss types of contracts for security services

HSCJ 202

MISM 661

▼ **5. Disposition of Classified Material**

- ▼ Explain the importance of remanence

HSCJ 202

MISM 661

- ▼ Explain the importance of the correct disposition of classified material

HSCJ 202

MISM 661

- ▼*Discuss disposition of classified materials

HSCJ 202

MISM 661

▼ **6. Facilities Planning**

- ▼ Explain the importance of facilities planning

HSCJ 202

MISM 661

- ▼*Discuss facilities planning

HSCJ 202

MISM 661

▼ **7. System Disposition/Reutilization**

- ▼*Explain the importance of vulnerabilities from improper disposition/reutilization

HSCJ 202

MISM 661

▼ **B. Life Cycle Management**

▼ **1. Life Cycle System Security Planning**

- ▼ Explain the importance of life cycle system security planning

HSCJ 202

MISM 661

- ▼*Discuss life cycle security planning

HSCJ 202

MISM 661

▼ **2. System Security Architecture**

- ▼ Explain how system security architecture supports continuity of operations CONOPS

HSCJ 202

MISM 661

- ▼*Discuss system security architecture

HSCJ 202
MISM 661

▼ **FUNCTION 6 - ASSIGN RESPONSIBILITIES**

▼ **N/A**

▼ **1. Certification and Accreditation (C&A)**

- ▼ Discuss roles associated with certification

HSCJ 202
MISM 661

- ▼ Explain importance of certification and accreditation (C&A)

HSCJ 202
MISM 661

- ▼ Facilitate the C&A process

HSCJ 202
MISM 661

- ▼*Discuss responsibilities associated with accreditation

HSCJ 202

▼ **2. Information Ownership**

- ▼*Explain the importance of establishing information ownership

HSCJ 202
MISM 661

▼ **3. System Certifiers and Accreditors**

- ▼*Discuss risk as it applies to certification and accreditation

HSCJ 202
MISM 661

▼ **4. Risk Analysts**

- ▼ Discuss systems certifiers and accreditors in risk mitigation

HSCJ 202
MISM 661

- ▼*Discuss risk analyst's reports

HSCJ 202
MISM 661

▼ **5. Information System Security Manager (ISSM)**

- ▼*Define the role of Information Assurance Manager (ISSM)

HSCJ 202
MISM 661

▼ **6. Information System Security Officer (ISSO)**

- ▼*Define the role of System Security Officer (ISSO)

HSCJ 202
MISM 661

▼ **FUNCTION 7 - DEFINE CRITICALITY AND SENSITIVITY**

▼ **N/A**

▼ **1. Aggregation**

- ▼*Explain the importance of the vulnerabilities associated with aggregation

HSCJ 202
MISM 661

▼ **2. Disclosure of Classified/Sensitive Information**

- ▼*Explain the liabilities associated with disclosure of classified/sensitive information

HSCJ 202
MISM 661

▼ **FUNCTION 8 - ALLOCATE RESOURCES**

▼ **N/A**

▼ **1. Resource Roles and Responsibilities**

- ▼ Assign/appoint key resource managers

HSCJ 202
MISM 661

- ▼*Discuss the respective roles and responsibilities of resource management staff

HSCJ 202
MISM 661

▼ **2. Budget/Resource Allocation**

- ▼ Defend the budget for information assurance

HSCJ 202
ISYS 411
MMBA 640
MISM 661

- ▼ Explain the importance of the information assurance budget

HSCJ 202
ISYS 411

- ▼*Evaluate the information assurance budget

HSCJ 202
ISYS 411
MMBA 640
MISM 661

▼ **3. Business Aspects of Information Security**

- ▼ Discuss protection of commercial proprietary information

HSCJ 202
MISM 661

- ▼ Explain the importance of business aspects of information security

HSCJ 202
MISM 665
MISM 661

- ▼ Explain the importance of protecting commercial proprietary information

HSCJ 202
MISM 661

- ▼*Discuss business aspects of information security

HSCJ 202
MISM 665
MISM 661

▼ **FUNCTION 9 - MULTIPLE AND JOINT ACCREDITATION**

▼ **N/A**

▼ **1. Memoranda of Understanding/Agreement (MOU/MOA)**

- ▼ Facilitate development and execution of MOU/MOA

HSCJ 202
MISM 661

- ▼*Explain the importance of MOU/MOA

HSCJ 202

▼ **FUNCTION 10 - ASSESS NETWORK SECURITY**

▼ **N/A**

▼ **1. Connectivity**

- ▼ Discuss connectivity involved in communications

HSCJ 202

MISM 670

MISM 661

- ▼ Explain the importance of connectivity involved in communications

HSCJ 202

MISM 670

MISM 661

- ▼ *Discuss connected organizations

HSCJ 202

MISM 670

MISM 661

▼ **2. Emissions Security (EMSEC) and TEMPEST**

- ▼ Discuss threats from Emissions Security (EMSEC)

HSCJ 202

MISM 661

- ▼ Discuss threats from TEMPEST failures

HSCJ 202

- ▼ Explain the importance of the threats from Emissions Security (EMSEC)

HSCJ 202

MISM 661

- ▼ Explain the importance of the threats from TEMPEST failures.

HSCJ 202

MISM 661

- ▼ *Define TEMPEST requirements

HSCJ 202

MISM 661

▼ **3. Wireless Technology**

- ▼ Discuss threats from electronic emanations

HSCJ 202

MISM 670

MISM 661

- ▼ Explain the importance of vulnerabilities associated with connected systems wireless technology

HSCJ 202

MISM 670

MISM 661

- ▼ Explain the importance of wireless technology

HSCJ 202

ISYS 325

MISM 670

- ▼ Explain the risks associated with portable wireless systems, viz., PDAs, etc.

HSCJ 202

MISM 670

HSCJ 315

MISM 661

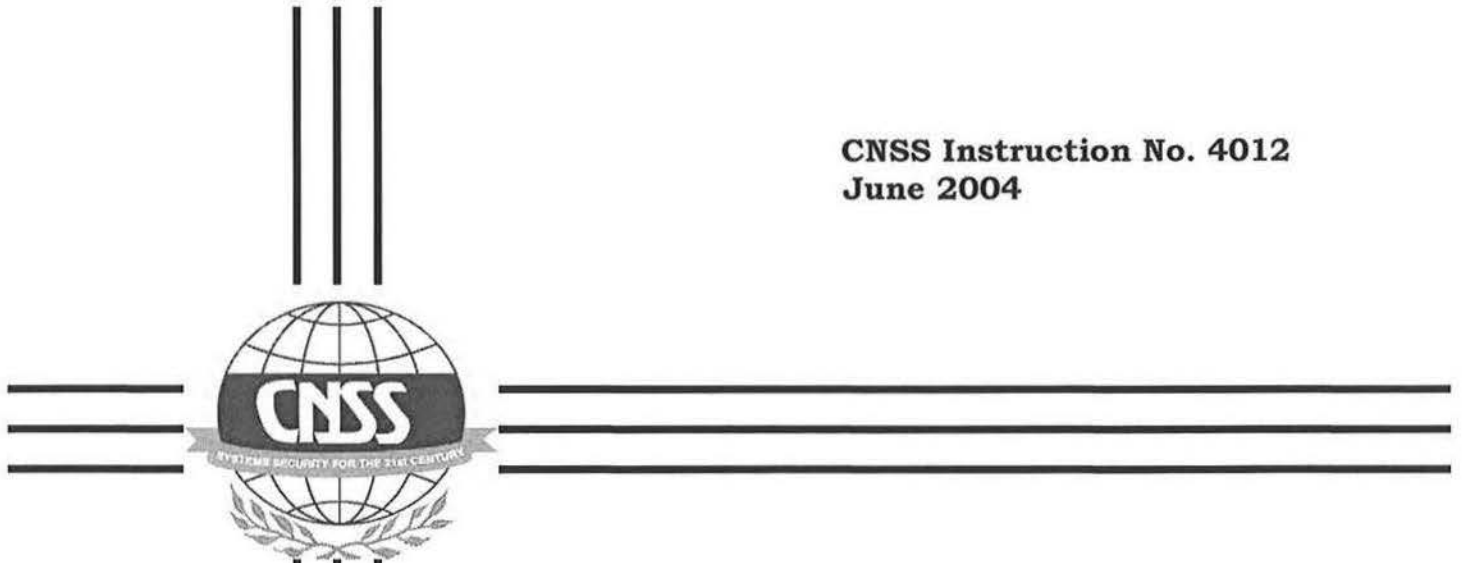
▼ *Discuss electronic emanations

HSCJ 202

MISM 670

MISM 661

b. Standard Specifications



**National Information Assurance
Training Standard
For
Senior System Managers**

Awareness, Training and Education (ATE) are cost-effective methods of improving organizational Information Assurance (IA). In times of ever-contracting budgets, it is difficult to persuade management to spend money on security and training activities that have no direct impact on the organizational bottom line. This paper describes the process used to aid in the systematic development of training to serve as the first line of defense in Information Assurance (IA). In addition it describes how these materials are applicable to your organizational long-range plans.

This document provides minimum standards for senior managers of national security systems. It also may offer guidelines for senior managers of unclassified systems. Your department or agency may require a more stringent implementation.



COMMITTEE ON NATIONAL SECURITY SYSTEMS

NATIONAL MANAGER

FOREWORD

1. Since the September 11th terrorist attacks against the sovereignty of the United States and its people, both the President and the Congress have redoubled their efforts to underpin the nation's security. The following guidance, reflecting their support, is intended to assist all federal agencies and private sector concerns in protecting their information systems. Only through diligence and a well-trained workforce will we be able to adequately defend the nation's vital information resources.

2. CNSSI No. 4012 is effective upon receipt. It replaces the National Training Standard for Designated Approving Authority (DAA), dated August 1997, which should be destroyed.

3. This instruction establishes the minimum course content or standard for the development and implementation of Information Assurance (IA) training for Senior Systems Managers (SSMs) of national security systems. Please check with your agency for applicable implementing documents.

4. Additional copies of this instruction can be obtained on the CNSS Website www.cnss.gov or by contacting the office at the address below:

NATIONAL SECURITY AGENCY
CNSS SECRETARIAT
ATTN: I01C STE 6716
FORT GEORGE G. MEADE, MD 20755-6716

/s/

MICHAEL V. HAYDEN
Lieutenant General, USAF

SENIOR SYSTEMS MANAGERS

NATIONAL IA TRAINING STANDARD FOR SENIOR SYSTEMS MANAGERS (SSMs)

	<u>SECTION</u>
PURPOSE	I
APPLICABILITY	II
RESPONSIBILITIES	III

SECTION I – PURPOSE

1. This instruction establishes the minimum standard for the development and implementation of Information Assurance (IA) training for Senior Systems Managers (SSM), *viz.*, Chief Information Officer (CIO), Designated Approving Authority (DAA), Chief Technology Officer (CTO), etc.

SECTION II – APPLICABILITY

2. The President’s National Strategy to Secure Cyberspace, Feb 03; National Security Telecommunications and Information Systems Security Directive (NSTISSD) No. 501, 16 Nov 92, and Federal Information Security Management Act (FISMA), 17 Dec 02, establish the requirements for federal departments and agencies to implement training programs for IA professionals. As defined in NSTISSD 501, an IA professional is an individual responsible for the security oversight or management of national security systems throughout all life-cycle phases. Those directives and others are being implemented in a synergistic environment among departments and agencies, which are committed to satisfying vigorously these IA education and training requirements. The following document is a continuation in a series of minimum training and education standards being developed to assist departments and agencies in meeting their responsibilities in these areas (CNSSI “old NSTISSI” Nos. 4011, 4013, 4014, 4015, and 4016). Implementing the training outlined in this document concomitantly will fulfill IA training requirements articulated in NIST Special Publication (SP) 800-16, and 5 Code of Federal Regulations (CFR) Part 930. The definitions for words used in this instruction are derived from the National Information Assurance (IA) Glossary, CNSSI No. 4009. Many references pertinent to this instruction may be found in ANNEX B.

3. The body of knowledge listed in this instruction was obtained from a variety of sources; *i.e.*, industry, government, and academia. ANNEX A lists the minimal IA performance standard for a SSM.

4. This instruction is applicable to all departments and agencies of the U.S. Government and their contractors responsible for the development and implementation of IA training for SSMs.

SECTION III – RESPONSIBILITIES

5. Heads of U.S. Government departments and agencies shall ensure that SSMs, *viz.*, CIOs, DAAs, CTOs, etc., are trained to the level of proficiency outlined in this instruction, and that such training is provided to those requiring it at the earliest practicable date.

6. The National Manager shall:

- a. maintain and provide an IA training standard for SSMs to U.S. Government departments and agencies;
- b. ensure that appropriate IA training courses for SSMs are developed;
- c. assist other U.S. Government departments and agencies in developing and/or conducting IA training activities for SSMs as requested; and
- d. maintain a national clearinghouse for training and education materials.

Enclosures:
ANNEX A
ANNEX B

ANNEX A

MINIMAL INFORMATION ASSURANCE (IA) PERFORMANCE STANDARD FOR SENIOR SYSTEMS MANAGERS (SSMs)

Job functions using competencies identified in:

- NSTISSI 1000, National Information Assurance Certification and Accreditation Process (NIACAP)
- NCSC-TG-027, Version 1, A Guide To Understanding Information System Security Officer Responsibilities For Automated Information Systems
- NCSC-TG-029, Version 1, Introduction to Certification and Accreditation
- FIPS Publication 102, Guideline for Computer Security Certification and Accreditation
- DODD 8000.1, Management of DoD Information Resources and Information Technology
- DODD 8500.1, Information Assurance
- DODI 8500.2, Information Assurance Implementation

TERMINAL OBJECTIVE:

Given a final report requesting approval to operate an information system at a specified level of trust, the SSM will analyze and judge the information for validity and reliability to ensure the system will operate at the proposed level of trust. This judgment will be predicated on an understanding of system architecture, system security measures, system operations policy, system security management plan, legal and ethical considerations, and provisions for system operator and end user training.

GENERAL BACKGROUND

The following items constitute a basic literacy necessary for Senior Systems Managers to proceed through the course material.

Definitions for SSMs	
Access authorization	Key management infrastructure
Access control policies	Law enforcement interfaces
Access controls	Law enforcement policies
Access controls – discretionary	Legal and liability issues as they apply to mission
Access controls – mandatory	Legal issues and Information Assurance (IA)
Access privileges	Legal issues which can affect Information Assurance (IA)
Accountability for sensitive data	Legal responsibilities of the SSM
Accreditation	Liabilities associated with disclosure of sensitive information
Accreditation procedure	Licensing
Accreditation types	Life cycle management
Administrative security policies	Life cycle security planning
Administrative security procedures	Life cycle system security planning
Aggregation	Logging policies
Approval to Operate (ATO) purpose and contents	Marking classified/sensitive information
Assignment of individuals to perform information assurance functions	Memorandum of Understanding/Agreement
Attacks	Methods of implementing risk mitigation strategies necessary to obtain ATO
Audit trail policy	Millennium Copyright Act
Auditable events	National Archives and Records Act
Automated countermeasures/deterrents	Need-to-know controls
Automated security tools	Non-repudiation
Availability (McCumber)	Operations Security
Background investigations	Organizational – threats
Backups	Organizational/agency information assurance emergency response teams
Biometric policies	Organizational/agency information assurance emergency response team role
Biometrics	Paperwork Reduction Act as codified in 44 U.S.C.A. Section 3501
Budget	Personnel security
Business recovery	Personnel security guidance
Certification	Personnel security policies
Certification and Accreditation effort leading to Systems Security Authorization Agreement	PKI
Certification and Accreditation process policy	Principles of aggregation
Certification procedure	Principles of information ownership
Certification roles	Principles of risk
Certification tools	Principles of system reconstitution
Certifiers understanding of mission	Privacy Act
Change control	Problems associated with disclosure of sensitive information

Clinger-Cohen Act	Procedural/administrative countermeasures
Commercial proprietary information	Protection profiles
Commercial proprietary information protection	Purpose of Systems Security Authorization Agreement (SSAA)
Common Criteria (Product Assurance) role in acquiring systems	Recertification
Communications Security (COMSEC) materials	Recertification effort
Computer crime and the various methods	Recertification of systems characteristics that need review
Computer Fraud and Abuse Act as codified in 18 U.S.C.A. Section 1030	Recertification process
Confidentiality (McCumber)	Recertification purpose
Configuration management	Reconstitution
Connected organizations	Recovery plan
Connectivity involved in communications	Remanence
Concept of Operations (CONOPS)	Residual risk
Contingency planning	Resources
Continuity of operations	Responsibilities associated with accreditation
Contracting for security services	Restoration
Copyright Act of 1976 and Copyright Amendment Act of 1992 as codified in 17 U.S.C.A	Restoration and continuity of operation
Copyright protection and license	Restoration process
Countermeasures	Results of certification tools
Countermeasures/deterrents – automated	Risk
Countermeasures/deterrents – technical	Risk acceptance
Criminal prosecution	Risk acceptance process
Declassification of media	Risk analysis
Delegation of authority	Role of risk analyst
Disaster recovery	Risk assessment
Disposition of classified material	Risk assessment as it supports granting waiver
Documentation	Risk assessment supporting granting an IATO
Documentation policies	Risk in certification and accreditation
Documentation role in reducing risk	Risk management
Downgrade of media	Risk mitigation
Due diligence	Risk mitigation strategies
Education, training, and awareness as a countermeasure	Risk mitigation strategies necessary to obtain IATO
Electronic emanations	Risk reports
Electronic records management	Risks associated with portable wireless systems, viz., PDAs etc.
Electronic-mail security	Risks from connectivity
Emergency destruction	Security Test, and Evaluation (ST&E) as part of acquisition process
Emergency destruction procedures	Separation of duties
Emissions Security (EMSEC)	Service Provider Exemption to the Federal Wiretap Statute [18 U.S.C.A. Section 2511(2)(a)(i)-(ii)]
Ethics	Storage (McCumber)
Evidence collection	System accreditors role
Evidence collection policies	System architecture
Evidence preservation	System certifiers role

Evidence preservation policies	System disposition
Execution of memoranda of understanding	System reutilization
Facilities planning	System security architecture
Federal Information Security Management Act (FISMA)	System security architecture support of continuity of operations (CONOPS)
Federal Property and Administration Service Act	Systems Security Authorization Agreement (SSAA)
Federal Records Act	TEMPEST failures
Fraud waste and abuse	TEMPEST requirements
Freedom of Information Act (FOIA) and Electronic Freedom of Information Act (EFOIA)	Test and evaluation
Government Information Security Reform Act (GISRA)	Threat
Government Paperwork Elimination Act (GPEA)	Threat analysis
Importance and role of non-repudiation	Threats – assessment
Importance and role of PKI	Threats – environmental
Importance of Security Test and Evaluation (ST&E) as part of acquisition process	Threats – human
Incident response	Threats – natural
Incident response policy	Threats from contracting for security services
Information Assurance (IA)	Threats to systems
Information assurance – SSM role	Transmission (McCumber)
Information assurance budget	Types of contracts for security services
Information assurance business aspects	Vulnerability
Information assurance cost benefit analysis	Vulnerability – aggregation
Information classification	Vulnerability – connected systems
Information ownership	Vulnerability – improper disposition
Information security policy	Vulnerability – improper reutilization
Interim approval to operate (IATO)	Vulnerability – network
Investigative authorities	Vulnerability – technical
Justification for waiver	Vulnerability – wireless technology

In each of the areas listed below, the SSM shall perform the following functions:

FUNCTION ONE - GRANT FINAL ATO

Granting final approval to operate an IS or network in a specified security mode

A. RESPONSIBILITIES

1. Aspects of Security
 - Explain the importance of SSM role in Information Assurance (IA)
2. Accreditation
 - Discuss accreditation
 - Discuss the certification process leading to successful accreditation
 - Explain the importance of accreditation
 - Explain types of accreditation
 - Facilitate the certification process leading to successful accreditation
 - Discuss the significance of NSTISSP No. 6

B. APPROVALS

1. Approval to Operate (ATO)
 - Explain ATO
 - Discuss purpose and contents of ATO
 - Explain the importance of risk assessment to support granting an ATO
2. Interim Approval to Operate (IATO)
 - Describe IATO
 - Explain the purpose and contents of IATO
 - Explain the importance of risk assessment to support granting an IATO
 - Facilitate implementation of risk mitigation strategies necessary to obtain IATO
3. Recertification
 - Describe recertification
 - Direct the recertification effort
 - Explain the importance of the recertification process
 - Identify characteristics of information systems that need re-certification
 - Initiate the recertification effort
4. Systems Security Authorization Agreement (SSAA)
 - Discuss the Systems Security Authorization Agreement (SSAA)
 - Explain the importance of the SSAA
5. Waive Policy to Continue Operation
 - Discuss justification for waiver
 - Discuss risk mitigation strategies necessary to obtain waiver
 - Ensure risk assessment supports granting waiver

FUNCTION TWO - REVIEW ACCREDITATION

Reviewing the accreditation documentation to confirm that the residual risk is within acceptable limits for each network and/or IS.

A. THREATS

1. Attacks
 - Discuss threats/attacks to systems
 - Explain the importance of threats/attacks on systems
2. Environmental/Natural Threats
 - Discuss environmental/natural threats
3. Human Threats
 - Explain the importance of intentional and unintentional human threats
4. Theft
 - Explain the importance of theft
5. Threat
 - Explain threat
 - Explain the importance of organizational threats
6. Threat Analysis
 - Explain the importance of threat analysis
7. Threat Assessment
 - Explain the importance of threat assessment

B. COUNTERMEASURES

1. Education, Training, and Awareness as Countermeasures
 - Explain the importance of educational training, and awareness as countermeasures
 - Ensure educational training, and awareness countermeasures are implemented
2. Procedural Countermeasures
 - Explain the importance of procedural/administrative countermeasures
 - Ensure procedural/administrative countermeasures are implemented
3. Technical Countermeasures
 - Explain the importance of automated countermeasures/deterrents
 - Explain the importance of technical countermeasures/deterrents
 - Ensure technical/automated countermeasures/deterrents are implemented

C. VULNERABILITY

1. Vulnerability
 - Explain vulnerability
2. Vulnerability Analysis
 - Explain the importance of vulnerability analysis

3. Network Vulnerabilities
 - Explain the importance of network vulnerabilities
4. Technical Vulnerabilities
 - Explain the importance of technical vulnerabilities

D. RISK MANAGEMENT

1. Cost/Benefit Analysis of Information Assurance
 - Explain the importance of cost/benefit analysis of information assurance
2. Documentation
 - Explain the importance of documentation role in reducing risk
3. Risk
 - Explain risk
 - Discuss principles of risk
4. Risk Assessment
 - Explain the importance of risk assessment
5. Risk Management
 - Explain the importance of risk management
6. Residual Risk
 - Explain residual risk
7. Risk Acceptance Process
 - Explain the importance of the risk acceptance process
8. Systems Security Authorization Agreement (SSAA)
 - Explain the importance of the certification and accreditation (C&A) effort leading to accreditation
 - Discuss the contents of SSAA
 - Discuss the purpose of SSAA
 - Ensure the certifier understands the mission and it is reflected in SSAA the C&A effort leading to SSAA
 - Facilitate effort leading to SSAA

FUNCTION THREE - VERIFY COMPLIANCE

Verifying that each information system complies with the information assurance (IA) requirements

A. LAWS RELATED TO INFORMATION ASSURANCE (IA) AND SECURITY

1. Copyright Protection and Licensing
 - Explain the importance of copyright protection
 - Explain the importance of licensing
2. Criminal Prosecution
 - Explain the importance of criminal prosecution
3. Due Diligence
 - Explain the importance of due diligence

4. Evidence Collection and Preservation
 - Explain the importance of evidence collection
 - Explain the importance of evidence preservation
5. Fraud, Waste, and Abuse
 - Explain fraud, waste, and abuse
6. Laws Related To Information Assurance and Security
 - Explain the importance of implications of Electronic Records Management and Federal Records Act
 - Explain the importance of implications of Federal Managers Financial Integrity Act of 1982
 - Explain the importance of implications of Federal Property and Administration Service Act
 - Explain the importance of implications of USA Patriot Act, GPEA, and Paperwork Reduction Acts
 - Explain the importance of implications of legal issues which can affect Information Assurance (IA)
 - Explain the importance of implications of National Archives and Records Act
 - Explain the importance of implications of the Computer Fraud and Abuse Act, P.L. 99- 474, 18 U.S. Code 1030
 - Explain the importance of implications of the Freedom of Information Act and Electronic Freedom of Information Act
 - Explain the importance of Public Law 107-347, E-Government Act of 2002, Title III, Federal Information Security Management Act (FISMA), 17 Dec 02
 - Explain the importance of implications of the legal responsibilities of senior systems managers.
 - Explain the importance of implications of the Privacy Act
 - Discuss implications of Public Law 107-347 regarding certification and accreditation
7. Legal and Liability Issues
 - Explain the importance of legal and liability issues as they apply to system and mission
8. Ethics
 - Discuss ethics

B. POLICY DIRECTION

1. Access Control Policies
 - Explain the importance of access control policies
2. Administrative Security Policies And Procedures
 - Explain the importance of administrative security policies/procedures
3. Audit Trails and Logging Policies
 - Explain the importance of audit trail policy
 - Explain the importance of logging policies
4. Documentation Policies
 - Explain the importance of documentation policies
5. Evidence Collection and Preservation Policies
 - Explain the importance of evidence collection/preservation policies

6. Information Security Policy
 - Define information security policy
 - Explain the importance of information security policy
7. National Information Assurance (IA) Certification & Accreditation (C&A) Process Policy
 - Explain the importance of the National Information Assurance (IA) Certification & Accreditation (C&A) Policy
8. Personnel Security Policies & Guidance
 - Explain the importance of personnel security guidance

C. SECURITY REQUIREMENTS

1. Access Authorization
 - Explain the importance of access authorization
2. Auditable Events
 - Explain auditable events
3. Authentication
 - Explain authentication
4. Background Investigations
 - Explain the importance of background investigations
5. Countermeasures
 - Explain the importance of countermeasures
6. Delegation of Authority
 - Discuss the importance of delegation of authority
 - Ensure that individuals are assigned to perform IA functions
7. Education, Training, and Awareness
 - Explain the importance of education, training, and awareness as countermeasures
 - Ensure educational, training, and awareness countermeasures are implemented
8. Electronic Records Management
 - Discuss electronic records management
 - Explain the importance of electronic records management
9. Electronic-Mail Security
 - Discuss electronic-mail security
 - Explain the importance of electronic-mail security
10. Information Classification
 - Discuss information classification
 - Explain the importance of information classification
11. Investigative Authorities
 - Discuss investigative authorities
 - Explain the importance of investigative authorities
12. Key Management Infrastructure
 - Discuss key management infrastructure
13. Information Marking
 - Discuss information marking

14. Non-repudiation
 - Discuss non-repudiation
 - Explain the importance and role of non-repudiation
15. Public Key Infrastructure (PKI)
 - Explain the importance and role of PKI

FUNCTION FOUR - ENSURE ESTABLISHMENT OF SECURITY CONTROLS

Ensuring the establishment, administration, and coordination of security for systems that agency, service, or command personnel or contractors operate

A. ADMINISTRATION

1. Accountability for Classified/Sensitive Data
 - Explain the importance of accountability for sensitive data
 - Discuss classification and declassification of information
2. Automated Security Tools
 - Explain the importance of automated security tools
3. Backups
 - Discuss backups
 - Explain the importance of backups
4. Change Control/Configuration Management
 - Discuss change control
 - Discuss configuration management
 - Explain the importance of configuration management
5. Declassification/Downgrade of Media
 - Explain the importance of downgrade of media
 - Discuss the importance of downgrade of information
6. Destruction/Purging/Sanitization of Classified/Sensitive Information
 - Explain the importance of destruction/purging/sanitization procedures for classified/sensitive information

B. ACCESS

1. Access Controls
 - Define manual/automated access controls
 - Explain the importance of manual/automated access controls
2. Access Privileges
 - Explain the importance of access privileges
3. Discretionary Access Controls
 - Discuss discretionary access controls
 - Explain the importance of discretionary access controls
4. Mandatory Access Controls
 - Define mandatory access controls
 - Explain the importance of mandatory access controls

5. Biometrics/Biometric Policies
 - Explain biometric policies
6. Separation of Duties
 - Define the need to ensure separation of duties where necessary
 - Explain the importance of the need to ensure separation of duties where necessary
7. Need-To-Know Controls
 - Define need to know controls
 - Explain the importance of need to know controls

C. INCIDENT HANDLING AND RESPONSE

1. Emergency Destruction Procedures
 - Explain the importance of emergency destruction procedures
2. Organizational/Agency Information Assurance Emergency Response Teams
 - Explain the role of organizational/agency information assurance emergency response teams

D. CONTINUITY OF OPERATIONS PLANNING

1. Business Recovery
 - Define business recovery
 - Explain the importance of business recovery
2. Contingency/Continuity of Operations Planning
 - Explain the importance of contingency/continuity of operations planning
 - Ensure the establishment and testing of contingency/continuity of operations plans
3. Disaster Recovery
 - Explain the importance of disaster recovery
4. Disaster Recovery Plan
 - Explain the importance of recovery plan
 - Ensure the establishment and testing of recovery plans
5. Incident response policies
 - Explain the importance of incident response policy
6. Law enforcement interfaces/policies
 - Discuss law enforcement interfaces
 - Discuss law enforcement policies
 - Explain the importance of law enforcement interfaces
7. Reconstitution
 - Define principles of system reconstitution
 - Explain the importance of principles of system reconstitution
8. Restoration
 - Explain the importance of restoration to continuity of operation

FUNCTION FIVE - ENSURE PROGRAM MANAGERS DEFINE SECURITY IN ACQUISITIONS

Ensuring that the Program Manager/Official defines the system security requirements for acquisitions

A. ACQUISITION

1. Certification Test & Evaluation (CT&E)
 - Define CT&E as part of acquisition process
 - Discuss the importance of CT&E as part of acquisition process
2. Certification Tools
 - Discuss significance/results of certification tools
3. Product Assurance
 - Explain the importance of product assurance role in acquiring systems, *i.e.*, NSTISSP No. 11, Jan 00
 - Explain the importance of protection profiles
 - Explain the importance of security targets
4. Contracting For Security Services
 - Discuss types of contracts for security services
 - Define where contracting for security services is appropriate
 - Explain threats from contracting for security services
5. Disposition of Classified Material
 - Discuss disposition of classified materials
 - Explain the importance of the correct disposition of classified material
 - Explain the importance of remanence
6. Facilities Planning
 - Discuss facilities planning
 - Explain the importance of facilities planning
7. System Disposition/Reutilization
 - Explain the importance of vulnerabilities from improper disposition/reutilization

B. LIFE CYCLE MANAGEMENT

1. Life Cycle System Security Planning
 - Discuss life cycle security planning
 - Explain the importance of life cycle system security planning
2. System Security Architecture
 - Discuss system security architecture
 - Explain how system security architecture supports continuity of operations CONOPS

FUNCTION SIX - ASSIGN RESPONSIBILITIES

Assigning Information Assurance (IA) responsibilities to the individuals reporting directly to the SSM

1. Certification and Accreditation (C&A)
 - Discuss responsibilities associated with accreditation
 - Discuss roles associated with certification
 - Explain importance of certification and accreditation (C&A)
 - Facilitate the C&A process
2. Information Ownership
 - Explain the importance of establishing information ownership
3. System Certifiers and Accreditors
 - Discuss risk as it applies to certification and accreditation
4. Risk Analysts
 - Discuss risk analyst's reports
 - Discuss systems certifiers and accreditors in risk mitigation
5. Information System Security Manager (ISSM)
 - Define the role of Information Assurance Manager (ISSM)
6. Information System Security Officer (ISSO)
 - Define the role of System Security Officer (ISSO)

FUNCTION SEVEN - DEFINE CRITICALITY AND SENSITIVITY

Defining the criticality and classification/sensitivity levels of each IS and approving the classification level required for the applications implemented on them

1. Aggregation
 - Explain the importance of the vulnerabilities associated with aggregation
2. Disclosure of Classified/Sensitive Information
 - Explain the liabilities associated with disclosure of classified/sensitive information

FUNCTION EIGHT - ALLOCATE RESOURCES

Allocate resources to achieve an acceptable level of security and to remedy security deficiencies

1. Resource Roles and Responsibilities
 - Discuss the respective roles and responsibilities of resource management staff
 - Assign/appoint key resource managers

2. Budget/Resource Allocation
 - Evaluate the information assurance budget
 - Explain the importance of the information assurance budget
 - Defend the budget for information assurance
3. Business Aspects of Information Security
 - Discuss business aspects of information security
 - Discuss protection of commercial proprietary information
 - Explain the importance of business aspects of information security
 - Explain the importance of protecting commercial proprietary information

FUNCTION NINE - MULTIPLE AND JOINT ACCREDITATION

Resolve issues regarding those systems requiring multiple or joint accreditation. This may require documentation of conditions or agreements in Memoranda of Agreement (MOA); and

1. Memoranda of Understanding/Agreement (MOU/MOA)
 - Explain the importance of MOU/MOA
 - Facilitate development and execution of MOU/MOA

FUNCTION TEN - ASSESS NETWORK SECURITY

Ensure that when classified/sensitive information is exchanged between IS or networks (internal or external), the content of this communication is protected from unauthorized observation, manipulation, or denial

1. Connectivity
 - Discuss connected organizations
 - Discuss connectivity involved in communications
 - Explain the importance of connectivity involved in communications
2. Emissions Security (EMSEC) and TEMPEST
 - Define TEMPEST requirements
 - Discuss threats from Emissions Security (EMSEC)
 - Discuss threats from TEMPEST failures
 - Explain the importance of the threats from Emissions Security (EMSEC)
 - Explain the importance of the threats from TEMPEST failures.
3. Wireless Technology
 - Discuss electronic emanations
 - Discuss threats from electronic emanations
 - Explain the importance of wireless technology
 - Explain the risks associated with portable wireless systems, *viz.*, PDAs, *etc.*
 - Explain the importance of vulnerabilities associated with connected systems wireless technology

ANNEX B

REFERENCES

The following references pertain to this instruction:






1. Common Criteria for Information Technology Security Evaluation, dtd Aug 99
2. DOD Directive 8000.1, Management of Information Resources and Information Technology, dtd 27 Feb 2002, *etc.*
3. DoD Directive 8500.1, Information Assurance, dtd 24 Oct 2002
4. DoD Directive 8500.1-M, Information Assurance Manual, (when effective)
5. DoD Instruction 8500.2, Information Assurance (IA) Implementation, dtd 6 Feb 2003
6. DOD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), dtd 30 Dec 1997
7. DoD 8510.1M, Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual, dtd 31 Jul 2000
8. EO 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, dtd 3 Apr 1984
9. E O 13231, Critical Infrastructure Protection in the Information Age, dtd 16 Oct 2001 as amended by EO 13286, Transfer of Certain Functions to the Secretary of Homeland Security, dtd 28 Feb 2003
10. Federal Information Processing Standards Publication (FIPS) Publication 31, Guidelines for Automatic Data Processing Physical Security and Risk Management, dtd Jun 1974
11. Federal Information Processing Standards Publication (FIPS) Publication 65, Guideline for Automatic Data Processing Risk Analysis, dtd 1 Aug 1993
12. Federal Information Processing Standards Publication (FIPS) 87, Guidelines for ADP Contingency Planning, dtd 27 Mar 1981
13. Federal Information Processing Standards Publication (FIPS) Publication 102, Guideline for Computer Security Certification and Accreditation, dtd 27 Sep 1983
14. National Computer Security Center (NCSC) TG-005, Trusted Network Interpretation (TNI), dtd 31 Jul 1987
15. National Computer Security Center (NCSC)-TG-027, Version 1, A Guide To Understanding Information System Security Officer Responsibilities for Automated Information Systems, dtd May 1992
16. National Computer Security Center (NCSC)-TG-029, Version 1, Introduction to Certification and Accreditation, dtd Jan 1994
17. NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, dtd Oct 1995
18. NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, dtd Sep 1996
19. NIST SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-based Model, dtd Apr 1998
20. NIST SP 800-18, Guide for Development of Security Plans for Information Technology Systems, dtd Dec 1998

21. NIST SP 800-64, Security Considerations in the Information Systems Development Life Cycle, dtd, Oct 2003
22. NSD 42, National Policy for the Security of National Security Telecommunications and Information Systems, dtd 5 Jul 1990
23. NSTISSD 501, National Training Program for Information Systems Security (INFOSEC) Professionals, dtd 16 Nov 1992
24. NSTISSI No.1000, National Information Assurance Certification and Accreditation Process (NIACAP), dtd Apr 2000
25. CNSSI No. 4009, National Information Assurance (IA) Glossary, dtd May 2003
26. NSTISSP No. 11, Revised Fact Sheet, National Assurance Information Acquisition Policy, dtd July 2003
27. OMB Circular No. A-130, Revised (Transmittal Memorandum No. 4), Management of Federal Information Resources, dtd 30 Nov 2000
28. OMB Memorandum M-00-07, Incorporating and Funding Security in Information Systems Investments, dtd 28 Feb 2000
29. OMB Memorandum M-01-08, Guidance on Implementing the Government Information Security Reform Act, dtd 16 Jan 2001
30. OMB Memorandum M-01-24, Reporting Instructions for the Government Information Security Reform Act, dtd 22 Jun 2001
31. OMB Memorandum M-02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones, dtd 17 Oct 2001
32. Code of Federal Regulations, 5 C.F.R. §903 *et seq.*, Employees Responsible for the Management or Use of Federal Computer Systems
33. PL 93-579, 5 U.S.C. §552a, the Privacy Act of 1974
34. PL 107-347, E-Government Act of 2002, Title III, Federal Information Security Management Act (FISMA), 17 Dec 2002
35. PL 104-106, Division E, the Information Technology Management Reform Act (Clinger-Cohen Act) of 1996
36. PL 106-398, Title X, Subtitle G, the Government Information Security Reform Act (GISRA)
37. The President's National Strategy to Secure Cyberspace, dtd Feb 2003

D. CNSS Standard NTSTISSI 4013

a. Course Mapping Details

b. Standard Specifications

 Print	 Collapse All	 Expand All	 Previous Page	 Next Page
---	--	--	---	--

Welcome Barbara Ciaramitaro, it is Monday, August 16, 2010 at 03:34:55 PM
You are currently viewing a report for CNSSI 4013 sorted by element.

▼ **FUNCTION 1 - SECURE USE**

▼ **A. General Security Policy**

▼ **1. Accountability**

- ▼ E - Outline accountability process/program

[HSCJ 202](#)

[MISM 661](#)

- ▼ *E - Define organizational accountability policies

[HSCJ 202](#)

[MISM 661](#)

▼ **2. Accreditation**

- ▼ *E - Define accreditation

[HSCJ 202](#)

[MISM 661](#)

▼ **3. Architecture**

- ▼ E - Address system security architecture study

[HSCJ 202](#)

[MISM 661](#)

- ▼ E - Identify appropriate security architecture for use in assigned IS

[HSCJ 202](#)

[MISM 661](#)

- ▼ *E - Define system security architecture

[HSCJ 202](#)

[MISM 661](#)

▼ **4. Assessment**

- ▼ *E - Define assessments for use during certification of information systems

[HSCJ 202](#)

[MISM 661](#)

▼ **5. Assurance**

- ▼ *E - Define assurance

[HSCJ 202](#)

[MISM 661](#)

▼ **6. Availability/Integrity/Confidentiality/Authentication/Non-repudiation**

- ▼ *E - Define concepts of availability, integrity, confidentiality, authentication, and non-repudiation

[HSCJ 202](#)

[MISM 661](#)

▼ **7. Certification**

- ▼ *E - Define certification policies as related to organizational requirements

[HSCJ 202](#)

[MISM 661](#)

▼ **8. NSTISSP 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA Enabled Information Technology (IT) Products**

- ▼*E - Identify NSTISSP 11 (Common Criteria) policies

HSCJ 202

MISM 661

▼ **9. Configuration Control**

- ▼*E - Define configuration control (management)

HSCJ 202

MISM 661

▼ **10. Custodian**

- ▼E - Identify information resource custodian

HSCJ 202

MISM 661

- ▼*E - Define resource custodian

HSCJ 202

MISM 661

▼ **11. Defense in Depth**

- ▼E - Give examples of defense in depth methods

HSCJ 202

MISM 661

- ▼E - Give examples of defense in depth policy

HSCJ 202

MISM 661

- ▼*E - Define defense in depth

HSCJ 202

MISM 661

▼ **12. Document**

- ▼*E - Identify DoDD 8500.1 policies (or appropriate civil agency guidance)

HSCJ 202

MISM 661

▼ **13. Domains**

- ▼E - Describe security domains as applicable to organizational policies

HSCJ 202

MISM 661

- ▼*E - Define security domains as applicable to organizational policies

HSCJ 202

MISM 661

▼ **14. E-Mail**

- ▼*E - Define organizational e-mail privacy policies

HSCJ 202

MISM 661

▼ **15. Wireless Security**

- ▼*E - Identify organizational wireless security policy

HSCJ 202

MISM 661

▼ **16. EMSEC/TEMPEST (Emanations Security/Short name referring to the investigation, study, and control of compromising emanations from IS equipment)**

- ▼ E - Describe EMSEC/TEMPEST control policies

HSCJ 202
MISM 661

- ▼ E - Identify EMSEC/TEMPEST control policies

HSCJ 202
MISM 661

- ▼ E - Identify EMSEC/TEMPEST security policies

HSCJ 202
MISM 661

- ▼ *E - Define EMSEC/TEMPEST security policies

HSCJ 202
MISM 661

▼ **18. FAX**

- ▼ *E - Describe relevant FAX security policies

HSCJ 202
MISM 661

▼ **19. Generally Accepted Security Principles**

- ▼ *E - Define generally accepted systems security principles

HSCJ 202
MISM 661

▼ **20. Goals/Mission/Objectives**

- ▼ *E - Define goals, mission, and objectives of the organization

HSCJ 202
MISM 665
MISM 661

▼ **21. Incident Response**

- ▼ *E - Describe incident response policies

HSCJ 202
HSCJ 210
MISM 661

▼ **22. Information Assurance**

- ▼ *E - Define organizational Information Assurance (IA) policies

HSCJ 202
MISM 661

▼ **23. Information Operations [DOD Organizations Only]**

- ▼ E - Describe information operations

HSCJ 202
MISM 661

- ▼ E - Support information operations

HSCJ 202
MISM 661

- ▼ *E - Define information operations

HSCJ 202
MISM 661

▼ **24. Internet Security**

- ▼*E - Describe organizational policies relevant to Internet security

HSCJ 202

MISM 661

▼ 25. Law Enforcement

- ▼E - Describe law enforcement interfaces

HSCJ 202

HSCJ 210

MISM 661

- ▼*E - Identify law enforcement interfaces

HSCJ 202

HSCJ 210

MISM 661

▼ 26. Marking

- ▼*E - Define policies relating to marking of classified, unclassified and sensitive information

HSCJ 202

MISM 661

▼ 27. Monitoring

- ▼E - Ensure legal aspects of monitoring are enforced

HSCJ 202

MISM 661

- ▼*E - Comply with legal aspects of monitoring

HSCJ 202

MISM 661

▼ 28. Multi-Level Security

- ▼E - Define fundamental concepts of multilevel security

HSCJ 202

- ▼E - Describe fundamental concepts of multilevel security

HSCJ 202

MISM 661

- ▼E - Identify fundamental concepts of multilevel security

HSCJ 202

MISM 661

- ▼*E - Describe multiple secure levels

HSCJ 202

MISM 661

▼ 29. Network

- ▼E - Describe policies relevant to network security

HSCJ 202

MISM 670

- ▼E - Describe wide area network (WAN) security policies

HSCJ 202

MISM 661

MISM 662

- ▼*E - Describe computer network defense

HSCJ 202

MISM 661

MISM 662

▼ **30. Operating System**

- ▼ *E - Define functional requirements for operating system integrity

HSCJ 202
MISM 670

▼ **32. Ownership**

- ▼ E - Identify information ownership of data held under his/her cognizance

HSCJ 202
MISM 661

- ▼ E - Identify information resource owner

HSCJ 202
MISM 661

- ▼ *E - Define information ownership of data held under his/her cognizance

HSCJ 202
MISM 661

▼ **33. Physical Security**

- ▼ *E - Define physical security

HSCJ 202
MISM 661

▼ **34. Records Management**

- ▼ E - Describe organizational security policies relative to electronic records management

HSCJ 202
MISM 661

- ▼ *E - Define records management

HSCJ 202
MISM 661

▼ **37. Security Tools**

- ▼ *E - Define automated security tools

HSCJ 202
MISM 661

▼ **38. Sensitivity**

- ▼ E - Describe information sensitivity in relation to organizational policies

HSCJ 202
MISM 661

- ▼ E - Explain information sensitivity

HSCJ 202
MISM 661

- ▼ *E - Define information sensitivity

HSCJ 202
MISM 661

▼ **39. Separation of Duties**

- ▼ E - Define organizational policies relating to separation of duties

HSCJ 202
MISM 661

- ▼ E - Explain separation of duties

HSCJ 202
MISM 661

- ▼*E - Define separation of duties

HSCJ 202
MISM 661

▼40. System Security

- ▼*E - Identify systems security standards policies

HSCJ 202
MISM 661

▼41. Information Technology Security Evaluation Criteria (ITSEC)

- ▼*E- Identify Information Security Technology Security Evaluation Criteria (ITSEC) policies

HSCJ 202
MISM 661

▼42. Testing

- ▼*E - Define testing policies

HSCJ 202
MISM 661

▼43. Validation/Verification

- ▼E - Identify verification and validation process policies

HSCJ 202
MISM 661

- ▼*E - Define validation policies

HSCJ 202
MISM 661

▼44. Workstation

- ▼*E - Describe workstation security policies

HSCJ 202
MISM 661

▼45. Zone

- ▼E - Define zoning

HSCJ 202
MISM 661

- ▼E - Describe zoning and zone of control policies

HSCJ 202
MISM 661

- ▼*E - Define zone of control

HSCJ 202
MISM 661

▼B. General Procedures

▼1. Network Software

- ▼E - Define transport layer security (i.e., secure socket layer [SSL])

HSCJ 202
ISYS 325
MISM 670

- ▼E - Define tunneling protocol (PPTP), layer 2 tunneling protocol (L2tp)

HSCJ 202
ISYS 325
MISM 670

- ▼ E - Define virtual private network (VPN) (i.e., SSH2, SOCKS)
 - HSCJ 202
 - ISYS 325
 - MISM 670
- ▼ E - Describe secure e-mail (i.e., PGP, S/MIME)
 - HSCJ 202
 - MISM 670
- ▼ E - Describe secure systems operations procedures
 - HSCJ 202
 - MISM 661
- ▼ E - Describe transport control protocol/internet protocol (TCP/IP)
 - HSCJ 202
 - ISYS 325
 - MISM 670
- ▼ E - Describe transport layer security (i.e., secure socket layer [SSL])
 - HSCJ 202
 - ISYS 325
 - MISM 670
- ▼ E - Describe tunneling protocol (PPTP), layer 2 tunneling protocol (l2tp)
 - HSCJ 202
 - ISYS 325
 - MISM 670
- ▼ E - Describe virtual private network (VPN) (i.e., SSH2, SOCKS)
 - HSCJ 202
 - ISYS 325
 - MISM 670
- ▼ *E - Define transport control protocol/internet protocol (TCP/IP)
 - HSCJ 202
 - ISYS 325
 - MISM 670
- ▼ **2. Aggregation**
 - ▼ E - Describe aggregation
 - HSCJ 202
 - MISM 670
 - ▼ *E - Define aggregation
 - HSCJ 202
 - MISM 670
- ▼ **3. Application Vulnerabilities**
 - ▼ E - Describe application and system vulnerabilities and threats -- client-based (i.e., applets, active-X)
 - HSCJ 202
 - MISM 661
 - ▼ E - Describe application and system vulnerabilities and threats -- mainframe
 - HSCJ 202
 - MISM 661
 - ▼ E - Describe application and system vulnerabilities and threats -- malicious code (i.e., Trojan horses, trap doors, viruses, worms)

HSCJ 202

MISM 661

- ▼ E - Describe application and system vulnerabilities and threats -- server-based

HSCJ 202

MISM 661

- ▼*E - Describe application and system vulnerabilities and threats -- web-based (i.e., XML, SAML)

HSCJ 202

MISM 661

▼ 4. Architecture

- ▼*E - Address system security architecture study

HSCJ 202

MISM 661

▼ 5. Assessment

- ▼*E - Prepare assessments for use during certification of information systems

HSCJ 202

MISM 661

▼ 7. Organizational/Agency Systems Emergency Response Team

- ▼ E - Report security issues to organizational/agency systems emergency response team

HSCJ 202

MISM 661

- ▼*E - Identify organizational/agency systems emergency response team

HSCJ 202

MISM 661

▼ 8. Database

- ▼ E - Define databases and data warehousing vulnerabilities, threats and protections

HSCJ 202

MISM 610

MISM 740

ISYS 200

- ▼ E - Describe data mining

MISM 740

STQM 342

- ▼ E - Describe databases and data warehousing vulnerabilities, threats and protections

HSCJ 202

MISM 610

MISM 740

- ▼*E - Define data mining

MISM 610

MISM 740

STQM 342

▼ 9. EMSEC/TEMPEST

- ▼ E - Identify certified EMSEC/TEMPEST technical authority (CTTA)

HSCJ 202

MISM 661

- ▼ E - Identify EMSEC/TEMPEST security procedures

HSCJ 202

MISM 661

- ▼*E - Define EMSEC/TEMPEST security procedures

HSCJ 202

MISM 661

▼ **10. End Systems**

- ▼ E - Describe end systems (i.e., workstations, notebooks, PDA, smartphones, etc.)

ISYS 325

MISM 670

- ▼*E - Define end systems (i.e., workstations, notebooks, PDA [personal digital assistant], smartphones, etc.)

ISYS 325

MISM 670

▼ **11. Facility Management**

- ▼*E - Practice facility management procedures

HSCJ 202

MISM 661

▼ **12. FAX**

- ▼ E - Practice FAX security policies/procedures

HSCJ 202

MISM 661

- ▼*E - Describe FAX security policies/procedures

HSCJ 202

MISM 661

▼ **13. Housekeeping**

- ▼ E - Describe housekeeping procedures

HSCJ 202

MISM 661

- ▼ E - Perform housekeeping procedures

HSCJ 202

MISM 661

- ▼*E - Define housekeeping procedures

HSCJ 202

MISM 661

▼ **14. Inference**

- ▼ E - Describe Inference

HSCJ 202

MISM 610

- ▼*E - Define Inference

HSCJ 202

MISM 610

▼ **15. Information States**

- ▼ E - Describe information states procedures

HSCJ 202

MISM 610

MISM 661

- ▼*E - Define information states procedures

HSCJ 202

MISM 610

MISM 661

▼ **16. Internet**

- ▼ *E - Define Internet security procedures

HSCJ 202

MISM 670

MISM 661

▼ **17. Investigations**

- ▼ *E - Assist in investigations as requested

HSCJ 202

HSCJ 210

▼ **18. IPSEC**

- ▼ E - Describe IPSEC authentication and confidentiality

HSCJ 202

MISM 661

- ▼ *E - Define IPSEC authentication and confidentiality

HSCJ 202

MISM 661

▼ **19. Marking**

- ▼ *E - Perform marking of sensitive information procedures (defined in C.F.R. 32 Section 2003, National Security Information - Standard Forms) as an example

HSCJ 202

MISM 661

▼ **20. Multi-Level Security**

- ▼ *E - Define multilevel security

HSCJ 202

MISM 661

▼ **21. Network, General**

- ▼ E - Define network components (hardware, firmware, software, and media)

ISYS 325

MISM 670

- ▼ E - Define network layer security

HSCJ 202

MISM 670

- ▼ E - Define network protocols

ISYS 325

MISM 670

- ▼ E - Define network types

HSCJ 202

ISYS 325

MISM 670

- ▼ E - Define wireless security

HSCJ 202

MISM 670

- ▼ E - Describe network architecture/topologies (i.e., ETHERNET, FDDI, bus, star, mesh, etc.)

HSCJ 202

ISYS 325

MISM 670

- ▼ E - Describe network components (hardware, firmware, software, and media)

ISYS 325

MISM 670

- ▼ E - Describe network layer security

HSCJ 202

MISM 670

MISM 661

- ▼ E - Describe network protocols

HSCJ 202

ISYS 325

MISM 670

- ▼ E - Describe network types

HSCJ 202

ISYS 325

MISM 670

- ▼ E - Describe WAN security procedures

HSCJ 202

MISM 670

- ▼ E - Describe wireless security

HSCJ 202

MISM 670

- ▼ E - Discuss network architecture/topologies (i.e., ETHERNET, FDDI, bus, star, mesh, etc.)

ISYS 325

MISM 670

- ▼ E - Practice WAN security procedures

HSCJ 202

MISM 670

- ▼ *E - Define network architecture/topologies (i.e., ETHERNET, FDDI, bus, star, mesh, etc.)

ISYS 325

MISM 670

▼ 22. Network Hardware

- ▼ E - Define concentrators

ISYS 325

MISM 670

- ▼ E - Define front-end processors, hubs, modems, multiplexers

ISYS 325

MISM 670

- ▼ E - Define gateways and routers

ISYS 325

MISM 670

- ▼ E - Define patch panels

ISYS 325

MISM 670

- ▼ E - Define routers
 - ISYS 325
 - MISM 670
- ▼ E - Define switches
 - ISYS 325
 - MISM 670
- ▼ E - Describe cable characteristics (i.e., twisted pair, fiber)
 - ISYS 325
 - MISM 670
- ▼ E - Describe concentrators
 - ISYS 325
 - MISM 670
- ▼ E - Describe front-end processors, hubs, modems, multiplexers
 - ISYS 325
 - MISM 670
- ▼ E - Describe gateways and routers
 - ISYS 325
 - MISM 670
- ▼ E - Describe patch panels
 - ISYS 325
 - MISM 670
- ▼ E - Describe routers
 - ISYS 325
 - MISM 670
- ▼ E - Describe switches
 - ISYS 325
 - MISM 670
- ▼ E - Identify gateways and routers
 - ISYS 325
 - MISM 670
- ▼ *E - Define cable characteristics (i.e., twisted pair, fiber)
 - ISYS 325
 - MISM 670
- ▼ **23. Network Software**
 - ▼ E - Define firewall technology (i.e., packet filtering, data inspection)
 - HSCJ 202
 - MISM 670
 - MISM 661
 - ▼ E - Define secure e-mail (i.e., PGP, S/MIME)
 - HSCJ 202
 - MISM 661
 - ▼ E - Describe firewall architecture (i.e., bastion host, DMZ)
 - HSCJ 202
 - MISM 670
 - MISM 661
 - ▼ E - Describe firewall technology (i.e., packet filtering, data inspection)

HSCJ 202

MISM 670

MISM 661

- ▼ E - Describe secure e-mail (i.e., PGP, S/MIME)

HSCJ 202

MISM 670

MISM 661

- ▼ E - Identify firewall architecture (i.e., bastion host, DMZ)

HSCJ 202

MISM 670

MISM 661

- ▼ E - Identify firewall technology (i.e., packet filtering, data inspection)

HSCJ 202

MISM 670

MISM 661

- ▼ E - Identify secure e-mail (i.e., PGP, S/MIME)

HSCJ 202

MISM 670

MISM 661

- ▼ *E - Define firewall architecture (i.e., bastion host, DMZ)

HSCJ 202

MISM 670

MISM 661

▼ 24. Objects

- ▼ E - Define polyinstantiation

HSCJ 202

MISM 610

- ▼ E - Describe object reuse

HSCJ 202

MISM 610

- ▼ E - Describe polyinstantiation

HSCJ 202

MISM 610

- ▼ *E - Define object reuse

HSCJ 202

MISM 610

▼ 25. Operating System

- ▼ E - Describe operating system integrity procedures

HSCJ 202

MISM 670

MISM 661

- ▼ E - Perform operating systems security procedures

HSCJ 202

MISM 670

MISM 661

- ▼ *E - Define operating systems security procedures

HSCJ 202

MISM 670

MISM 661

▼ **26. OSI (Open Systems Interconnect)**

- ▼ E - Define data link layer security

HSCJ 202

MISM 661

- ▼ E - Define network layer security

HSCJ 202

MISM 661

- ▼ E - Define OSI model

HSCJ 202

MISM 661

- ▼ E - Define transport control protocol/ internet protocol (TCP/IP)

HSCJ 202

ISYS 325

MISM 670

MISM 661

- ▼ E - Define transport layer security (i.e., secure socket layer [SSL])

HSCJ 202

MISM 661

- ▼ E - Define tunneling protocol (PPTP), layer 2 tunneling protocol (l2tp)

HSCJ 202

MISM 670

MISM 661

- ▼ E - Describe application layer security protocols (i.e., secure electronic transactions, secure hypertext, secure remote procedure call)

HSCJ 202

MISM 670

MISM 661

- ▼ E - Describe data link layer security

HSCJ 202

MISM 661

- ▼ E - Describe network layer security

HSCJ 202

MISM 661

- ▼ E - Describe OSI model

HSCJ 202

MISM 661

- ▼ E - Describe physical layer

HSCJ 202

MISM 661

- ▼ E - Describe presentation layer

HSCJ 202

MISM 661

- ▼ E - Describe session layer

HSCJ 202

MISM 661

- ▼ E - Describe transport control protocol/ internet protocol (TCP/IP)

HSCJ 202

ISYS 325

MISM 670

MISM 661

- ▼ E - Describe transport layer security (i.e., secure socket layer [SSL])

HSCJ 202

MISM 661

- ▼ *E - Define application layer security protocols (i.e., secure electronic transactions, secure hypertext, secure remote procedure call)

HSCJ 202

MISM 661

▼ 27. Rainbow Series

- ▼ *E - Describe purpose and contents of National Computer Security Center TG-005, Trusted Network Interpretation (TNI) or Red Book as examples

HSCJ 202

MISM 661

▼ 28. NSTISSAM COMPUSEC/1-99

- ▼ *E - Describe purpose and contents of NSTISSAM COMPUSEC/1-99, Advisory Memorandum on the Transition from the Trusted Computer System Evaluation Criteria to the International Common Criteria for Information Technology Security Evaluation

HSCJ 202

MISM 661

▼ 29. Security Procedures

- ▼ E - Assist in organizational security procedures

HSCJ 202

MISM 661

- ▼ *E - Define organizational security procedures

HSCJ 202

MISM 661

▼ 30. Security tools

- ▼ E - Describe automated security tools

HSCJ 202

MISM 661

- ▼ *E - Define automated security tools

HSCJ 202

MISM 661

▼ 31. Vulnerability and Threat

- ▼ E - Address application and system vulnerabilities and threats -- client-based (i.e., applets, active-X)

HSCJ 202

MISM 661

- ▼ E - Address application and system vulnerabilities and threats -- malicious code (i.e., Trojan Horses, trap doors, viruses, worms)

HSCJ 202

MISM 661

- ▼ E - Address application and system vulnerabilities and threats -- server-based

HSCJ 202

MISM 661

- ▼ E - Address application and system vulnerabilities and threats -- web-based (i.e., XML, SAML)

HSCJ 202

MISM 661

- ▼ E - Define application and system vulnerabilities and threats -- client-based (i.e., applets, active-X)

HSCJ 202

MISM 661

- ▼ E - Define application and system vulnerabilities and threats -- mainframe

HSCJ 202

MISM 661

- ▼ E - Define application and system vulnerabilities and threats -- malicious code (i.e., Trojan Horses, trap doors, viruses, worms)

HSCJ 202

MISM 661

- ▼ E - Define application and system vulnerabilities and threats -- server-based

HSCJ 202

MISM 661

- ▼ E - Define application and system vulnerabilities and threats -- web-based (i.e., XML, SAML)

HSCJ 202

MISM 661

- ▼ E - Describe application and system vulnerabilities and threats -- client-based (i.e., applets, active-X)

HSCJ 202

MISM 661

- ▼ E - Describe application and system vulnerabilities and threats -- mainframe

HSCJ 202

MISM 661

- ▼ E - Describe application and system vulnerabilities and threats -- malicious code (i.e., Trojan Horses, trap doors, viruses, worms)

HSCJ 202

MISM 661

- ▼ E - Describe application and system vulnerabilities and threats -- server-based

HSCJ 202

MISM 661

- ▼ E - Describe application and system vulnerabilities and threats -- web-based (i.e., XML, SAML)

HSCJ 202

MISM 661

- ▼ *E - Address application and system vulnerabilities and threats - mainframe

HSCJ 202

MISM 661

▼ **C. General Awareness, Training and Education (AT&E)**

▼ **1. Awareness, Training and Education (AT&E)**

- ▼ E - Identify sources of AT&E materials

HSCJ 202
MISM 661

- ▼*E - Describe attack actions as training issues

HSCJ 202
MISM 661

▼ **D. General Countermeasures and Safeguards**

▼ **2. AT&E**

- ▼*E - Recognize awareness, training, and education (AT&E) as a countermeasure

HSCJ 202
MISM 661

▼ **3. Backup**

- ▼*E - Define backup critical information

HSCJ 202
MISM 661

▼ **4. COMSEC**

- ▼E - Identify organizational COMSEC manager (Custodian)

HSCJ 202
MISM 661

- ▼E - List national COMSEC policies

HSCJ 202
MISM 661

- ▼E - List national COMSEC procedures

HSCJ 202
MISM 661

- ▼*E - Identify national COMSEC manager (Custodian)

HSCJ 202
MISM 661

▼ **5. Countermeasures**

- ▼*E - Describe what is meant by countermeasures

HSCJ 202
MISM 661

▼ **6. Digest**

- ▼*E - Define message digests (i.e., MD5, SHA, HMAC)

HSCJ 202
MISM 670

▼ **7. Digital Signature**

- ▼*E - Define digital signatures

HSCJ 202
HSCJ 210
MISM 661

▼ **8. Due Care**

- ▼*E - Define due care (due diligence)

HSCJ 202
HSCJ 210
MISM 661

▼ **9. E-Mail**

- ▼E - Describe e-mail privacy safeguards

HSCJ 202

MISM 661

- ▼*E - Describe e-mail privacy countermeasures

HSCJ 202

MISM 661

▼ **10. EMSEC/TEMPEST**

- ▼ E - Define EMSEC/TEMPEST security safeguards

HSCJ 202

MISM 661

- ▼*E - Define EMSEC/TEMPEST security countermeasures

HSCJ 202

MISM 661

▼ **11. Facilities**

- ▼*E - Define facility support systems (i.e., fire protection and HVAC)

HSCJ 202

MISM 661

▼ **12. Hardware**

- ▼*E - Define computing and telecommunications hardware/software

HSCJ 202

ISYS 325

MISM 670

▼ **13. Internet**

- ▼*E - Define internet security

HSCJ 202

MISM 670

MISM 661

▼ **14. Key**

- ▼ E - Define key recovery

HSCJ 202

HSCJ 315

MISM 661

- ▼ E - Define key storage/destruction

HSCJ 202

HSCJ 315

MISM 661

- ▼ E - Define PKI (Public Key Infrastructure) requirements

HSCJ 202

HSCJ 315

MISM 661

- ▼ E - Submit requirements for key management within the system

HSCJ 202

HSCJ 315

MISM 661

- ▼*E - Define key creation/distribution

HSCJ 202

HSCJ 315

MISM 661

▼ **15. Legal**

- ▼*E - Define legal requirements
 - [HSCJ 202](#)
 - [HSCJ 315](#)
 - [MISM 661](#)
- ▼ **16. Marking**
 - ▼*E - Define marking, handling, storing, and destroying of classified, unclassified, and sensitive information & media
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **17. Media**
 - ▼E - Define marking, handling, storing, and destroying of sensitive information & media
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼E - Define media (i.e., tape, paper or disks) management
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼E - Define secure data deletion for media reuse
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼*E - Define magnetic media degaussing
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **18. Misuse**
 - ▼*E - Define resource misuse prevention
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **19. Non-Repudiation**
 - ▼*E - Define digital non-repudiation
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **20. Operations**
 - ▼*E - Describe information operations
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **21. Privacy**
 - ▼*E - Define privacy and protection
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **22. Privilege**
 - ▼E - Define operator/administrator privileges
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼*E - Define need-to-know/least privilege
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **23. Record**

- ▼*E - Define record retention
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **24. Safeguards**
 - ▼E - Describe what is meant by safeguards
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼*E - Define safeguards used to prevent software piracy
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **25. Separation of Duties**
 - ▼E - Explain separation of duties as a countermeasure
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼*E - Describe separation of duties as a countermeasure
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **26. Software Countermeasure**
 - ▼E - Define countermeasures used to prevent software piracy
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼*E - Define anti-virus systems
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **27. Testing**
 - ▼*E - Identify automated tools for security testing
 - [HSCJ 202](#)
 - [MISM 661](#)
 - [MISM 662](#)
- ▼ **28. Tools**
 - ▼E - Describe automated tools for security test
 - [HSCJ 202](#)
 - [MISM 661](#)
 - [MISM 662](#)
 - ▼*E - Describe automated tools for security compliance
 - [HSCJ 202](#)
 - [MISM 661](#)
 - [MISM 662](#)
- ▼ **E. Administrative Countermeasures/Safeguards**
 - ▼ **1. Alarm**
 - ▼E - Identify alarms, signals and reports
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼E - Implement alarms, signals and reports
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼*E - Describe alarms, signals and reports

HSCJ 202
MISM 661

▼ **2. Assessment**

- ▼ E - Prepare assessments for use during certification of information systems

HSCJ 202
MISM 661

- ▼ *E - Assist in preparing assessments

HSCJ 202
MISM 661

▼ **3. System Test and Evaluation (ST&E)**

- ▼ E - Recommend revisions to System Test and Evaluation (ST&E) Plan and Procedures

HSCJ 202
MISM 661

- ▼ *E - Discuss System Test and Evaluation (ST&E) Plan and Procedures

HSCJ 202
MISM 661

▼ **4. Audit**

- ▼ *E - Identify audit collection requirements

HSCJ 202
MISM 661

▼ **5. Certification**

- ▼ E - Identify certification tools

HSCJ 202
MISM 661

- ▼ E - Recommend use of specific certification tools

HSCJ 202
MISM 661

- ▼ *E - Discuss certification tools

HSCJ 202
MISM 661

▼ **6. Control**

- ▼ E - Define system software controls

HSCJ 202
MISM 661

- ▼ E - Differentiate security-related changes from non-security-related changes

HSCJ 202
MISM 661

- ▼ E - Identify storage media protection and control

HSCJ 202
MISM 661

- ▼ *E - Define application development control

HSCJ 202
MISM 661

▼ **7. Countermeasures**

- ▼ *E - Identify countermeasures

HSCJ 202

MISM 661

▼ **12. Password**

- ▼ E - Define password management

HSCJ 202

MISM 661

- ▼ E - Identify password management systems

HSCJ 202

MISM 661

- ▼ *E - Address password management with staff

HSCJ 202

MISM 661

▼ **14. Recovery**

- ▼ E - Describe disaster recovery procedures

HSCJ 202

MISM 661

- ▼ *E - Address recovery procedures with staff

HSCJ 202

MISM 661

▼ **16. Separation of Duties**

- ▼ E - Evaluate separation of duties

HSCJ 202

MISM 661

- ▼ E - Implement separation of duties

HSCJ 202

MISM 661

- ▼ *E - Define separation of duties

HSCJ 202

MISM 661

▼ **F. Operations Policies/Procedures**

▼ **1. Assessment**

- ▼ *E - Support assessments for use during certification of information systems

HSCJ 202

MISM 661

▼ **2. Countermeasures**

- ▼ E - List protective technologies

HSCJ 202

MISM 661

- ▼ *E - Identify protective technologies

HSCJ 202

MISM 661

▼ **3. Crime**

- ▼ *E - Support anti-criminal activity preparedness planning (law enforcement)

HSCJ 202

HSCJ 210

ISIN 330

MISM 661

▼ **5. Disposition**

- ▼ *E - Identify disposition of media and data policies and procedures

HSCJ 202
MISM 661

▼ **6. Documentation**

- ▼ *E - Describe documentation policy and procedures

HSCJ 202
MISM 661

▼ **7. Media**

- ▼ E - Identify storage media protection policies and procedures

HSCJ 202
MISM 661

- ▼ *E - Identify storage media control policies and procedures

HSCJ 202
MISM 661

▼ **9. Privacy**

- ▼ *E - Outline known means of keystroke monitoring

HSCJ 202
MISM 661

▼ **10. Recovery**

- ▼ E - Describe disaster recovery policies and procedures

HSCJ 202
MISM 661

- ▼ *E - Define disaster recovery policies and procedures

HSCJ 202
MISM 661

▼ **11. Separation of Duties**

- ▼ *E - Describe separation of duties policies and procedures

HSCJ 202
MISM 661

▼ **12. Vendor**

- ▼ E - Explain vendor cooperation

HSCJ 202
ISYS 411
MMBA 640

- ▼ *E - Facilitate vendor cooperation

HSCJ 202
ISYS 411
MMBA 640

▼ **G. Contingency/Continuity of Operations**

▼ **1. Backup**

- ▼ *E - Outline security policy for backup procedures

HSCJ 202
MISM 661

▼ **3. Continuity/Contingency**

- ▼ E - Prepare input to continuity/contingency plan

HSCJ 202

MISM 661

- ▼*E - Describe continuity/contingency planning

HSCJ 202

MISM 661

▼ **4. Recovery**

- ▼ E - Describe disaster recovery plan testing

HSCJ 202

MISM 661

- ▼ E - Prepare input to recovery plan

HSCJ 202

MISM 661

- ▼*E - Describe disaster recovery

HSCJ 202

MISM 661

▼ **FUNCTION 2 - INCIDENTS**

▼ **A. Policy and Procedures**

▼ **2. Disposition**

- ▼*E - Address disposition procedures with staff

HSCJ 202

MISM 661

▼ **3. Due Care**

- ▼*E - Address questions from users about due care

HSCJ 202

MISM 661

▼ **4. Incident**

- ▼ E - Address unauthorized access incident reporting with staff

HSCJ 202

MISM 661

- ▼ E - Define breaches

HSCJ 202

HSCJ 210

MISM 661

- ▼ E - Define incident response

HSCJ 202

MISM 661

- ▼*E - Define incidents

HSCJ 202

HSCJ 210

MISM 661

▼ **5. Intrusion**

- ▼ E - Address intrusion detection management with staff

HSCJ 202

MISM 661

- ▼*E - Define intrusion detection

HSCJ 202

MISM 661

▼ **6. Legal**

- ▼ E - Assist in evidence identification/preservation

HSCJ 202
HSCJ 210
MISM 661

- ▼ *E - Assist appropriate authority in witness interviewing/interrogation

HSCJ 202
HSCJ 210
MISM 661

▼ **7. Reporting**

- ▼ *E - Define reporting

HSCJ 202
MISM 661

▼ **9. Violation**

- ▼ *E - Define violations

HSCJ 202
MISM 661

▼ **B. Operations Countermeasures/Safeguard**

▼ **2. Attack**

- ▼ *E - Identify an attack

HSCJ 202
HSCJ 210
MISM 661

▼ **4. Authentication**

- ▼ *E - Address work force about authentication procedures

HSCJ 202
MISM 661

▼ **5. Organizational/Agency Systems Emergency Response Team**

- ▼ *E - Describe the organizational/agency systems emergency/incident response team

HSCJ 202
HSCJ 210
MISM 661

▼ **6. Countermeasure**

- ▼ E - Describe countermeasures

HSCJ 202
MISM 661

- ▼ *E - Assist in performing countermeasure/safeguard corrective actions

HSCJ 202
MISM 661

▼ **7. Incident**

- ▼ E - Assist in incident response

HSCJ 202
HSCJ 210
MISM 661

- ▼ *E - Address unauthorized access incident reporting with staff

HSCJ 202
HSCJ 210
MISM 661

▼ **9. Legal**

- ▼ *E - Assist appropriate authority in witness interviewing/interrogation

HSCJ 202
HSCJ 210
MISM 661

▼ **10. Safeguard**

- ▼ *E - Describe safeguards

HSCJ 202
MISM 661

▼ **C. Contingency Countermeasures/Safeguards**

▼ **2. Availability**

- ▼ *E - Define information availability

HSCJ 202
MISM 661

▼ **3. Correction**

- ▼ *E - Identify examples of corrective actions

HSCJ 202
MISM 661

▼ **5. Incident**

- ▼ *E - Address unauthorized access incident reporting with staff

HSCJ 202
HSCJ 210
MISM 661

▼ **6. Intrusion**

- ▼ *E - Identify methods of intrusion detection

HSCJ 202
MISM 661

▼ **FUNCTION 3 - CONFIGURATION**

▼ **A. Administrative Policies/Procedures**

▼ **3. Authentication**

- ▼ E - Address work force about authentication procedures

HSCJ 202
MISM 661

- ▼ *E - Address authentication with staff

HSCJ 202
MISM 661

▼ **4. Biometrics**

- ▼ *E - Address biometric access management with staff

HSCJ 202
MISM 661

▼ **5. Organizational/Agency Systems Emergency/Incident Response Team**

- ▼ *E - Identify organizational/agency systems emergency/incident response team

HSCJ 202
HSCJ 210
MISM 661

▼ **6. Configure**

- ▼ E - Address configuration management with staff

HSCJ 202

MISM 661

- ▼ E - Address staff about legal configuration restrictions

HSCJ 202

MISM 661

- ▼ E - Adhere to configuration control

HSCJ 202

MISM 661

- ▼ E - Define configuration control

HSCJ 202

MISM 661

- ▼ E - Monitor configuration control

HSCJ 202

MISM 661

- ▼ *E - Define change control policies

HSCJ 202

MISM 661

▼ **7. Copyright**

- ▼ E - Define copyright protection and licensing

HSCJ 202

MISM 661

- ▼ *E - Adhere to copyright protection and licensing

HSCJ 202

MISM 661

▼ **10. Install/Patch**

- ▼ *E - Identify appropriate sources for updates and patches

HSCJ 202

MISM 661

▼ **12. Management**

- ▼ *E - Identify basic/generic management issues

HSCJ 202

MISM 665

MISM 661

▼ **15. Operation**

- ▼ *E - Define operational procedure review

HSCJ 202

MISM 661

▼ **16. Password**

- ▼ *E - Address password management with staff

HSCJ 202

MISM 661

▼ **FUNCTION 4 - ANOMALIES AND INTEGRITY**

▼ **A. General Risk Management**

▼ **1. Attack**

- ▼ E - Identify attack actions

HSCJ 202

MISM 661

MISM 662

- ▼*E - Describe attack actions

HSCJ 202

MISM 661

▼3. EMSEC/TEMPEST

- ▼ E - Describe EMSEC/TEMPEST security as it relates to the risk management process

HSCJ 202

MISM 661

- ▼*E - Define EMSEC/TEMPEST security as it relates to the risk management process

HSCJ 202

MISM 661

▼4. Internet

- ▼*E - Describe ways to provide protection for Internet connections

HSCJ 202

MISM 670

MISM 661

▼5. Legal

- ▼*E - Assist in investigations as requested

HSCJ 202

HSCJ 210

MISM 661

▼6. Logging

- ▼*E - Describe the different categories of activities which may be logged

HSCJ 202

MISM 661

▼7. Network

- ▼ E - Describe LAN/WAN security

HSCJ 202

MISM 670

- ▼*E - Describe wireless security

HSCJ 202

MISM 670

▼8. Operating System

- ▼*E - Describe operating system integrity

HSCJ 202

MISM 670

▼10. Threat

- ▼*E - Identify different types of threat

HSCJ 202

MISM 661

MISM 662

▼11. Zone

- ▼*E - Describe on what zoning and zone of control ratings are based

HSCJ 202

MISM 670

▼B. Access Control Safeguards

▼ **1. Access Control**

- ▼ E - Address work force about access control software management procedures
HSCJ 202
MISM 661
- ▼ E - Define decentralized/distributed -- single sign on (SSO) (i.e., Kerberos)
HSCJ 202
MISM 661
- ▼ E - Define discretionary access controls
HSCJ 202
MISM 661
- ▼ E - Define mandatory access controls
HSCJ 202
MISM 661
- ▼ E - Define security domain
HSCJ 202
MISM 661
- ▼ E - Describe access control physical, logical, and administrative configurations
HSCJ 202
MISM 661
- ▼ E - Describe access rights and permissions
HSCJ 202
MISM 661
- ▼ E - Describe control techniques and policies (i.e., discretionary, mandatory, and rule of least privilege)
HSCJ 202
MISM 661
- ▼ E - Identify access control attacks (brute force, dictionary, spoofing, denial of service, etc.)
HSCJ 202
MISM 661
- ▼ *E - Address access control software management with staff
HSCJ 202
MISM 661

▼ **2. Alarms**

- ▼ *E - Demonstrate the ability to use alarms, signals, and reports
HSCJ 202
MISM 661

▼ **3. Authentication**

- ▼ E - Describe identification and authentication techniques
HSCJ 202
MISM 661
- ▼ E - Identify identification and authentication techniques
HSCJ 202
MISM 661
- ▼ *E - Describe centralized/remote authentication access controls
HSCJ 202
MISM 661

▼ **4. Distribution System**

- ▼*E - Define protected distribution systems

[HSCJ 202](#)

[MISM 661](#)

▼ **6. Legal**

- ▼E - Assist in investigations as requested

[HSCJ 202](#)

[HSCJ 210](#)

[MISM 661](#)

- ▼*E - Address staff about legal access restrictions

[HSCJ 202](#)

[MISM 661](#)

▼ **7. Monitor**

- ▼E - Describe accountability and monitoring (i.e., correction, alarms, audit trail)

[HSCJ 202](#)

[MISM 661](#)

- ▼*E - Define accountability and monitoring (i.e., correction, alarms, audit trail)

[HSCJ 202](#)

[MISM 661](#)

▼ **8. Network**

- ▼*E - Identify network security software

[HSCJ 202](#)

[MISM 670](#)

[MISM 661](#)

▼ **9. Operating System**

- ▼*E - Describe operating system security features

[HSCJ 202](#)

[MISM 670](#)

[MISM 661](#)

▼ **10. Ownership**

- ▼*E - Describe data ownership and custodianship

[HSCJ 202](#)

[MISM 661](#)

▼ **11. Safeguards**

- ▼*E - Describe system security safeguards

[HSCJ 202](#)

[MISM 670](#)

[MISM 661](#)

▼ **C. Audit Policies and Procedures**

▼ **1. Address**

- ▼*E - Address access management with staff

[HSCJ 202](#)

[MISM 661](#)

▼ **4. Legal**

- ▼E - Assist in investigations as requested

[HSCJ 202](#)

[HSCJ 210](#)

[MISM 661](#)

- ▼*E - Address staff about legal access restrictions

HSCJ 202

MISM 661

▼ **6. Separation of Duties**

- ▼ *E - Describe situations in which separation of duties is appropriate or mandatory

HSCJ 202

MISM 661

▼ **D. Audit Countermeasures/Safeguards**

▼ **2. Legal**

- ▼ *E - Assist in investigations as requested

HSCJ 202

HSCJ 210

MISM 661

▼ **E. Audit Tools**

▼ **1. Audit**

- ▼ E - Describe the major benefit gained through use of audit trails and logging policies

HSCJ 202

MISM 661

- ▼ E - Identify audit tools

HSCJ 202

MISM 661

- ▼ *E - Define an error/audit log

HSCJ 202

MISM 661

▼ **2. Intrusion**

- ▼ *E - Identify intrusion detection systems

HSCJ 202

MISM 661

▼ **3. Legal**

- ▼ *E - Assist in investigations as requested

HSCJ 202

HSCJ 210

MISM 661

▼ **4. Operating Systems**

- ▼ *E - Describe major operating system security features

HSCJ 202

MISM 670

▼ **F. Operations Management/Oversight**

▼ **3. Configuration Management**

- ▼ *E - Describe configuration management

HSCJ 202

MISM 661

▼ **5. Legal**

- ▼ *E - Assist in investigations as requested

HSCJ 202

HSCJ 210

MISM 661

▼ **6. Monitoring**

- ▼*E - Address monitoring management with staff

HSCJ 202
MISM 661

▼ **8. Recovery**

- ▼E - Describe disaster recovery oversight

HSCJ 202
MISM 661

- ▼*E - Describe disaster recovery management

HSCJ 202
MISM 661

▼ **G. Configuration Management**

▼ **5. Legal**

- ▼*E - Assist in investigations as requested

HSCJ 202
HSCJ 210
MISM 661

▼ **6. Media**

- ▼*E - Identify storage media protection and control procedures

HSCJ 202
MISM 661

▼ **7. Subjects and Objects**

- ▼*E - Define subjects and objects

HSCJ 202
MISM 661

▼ **10. Trusted Computer Base (TCB)**

- ▼*E - Define trusted computer base (TCB) reference monitors and kernels

HSCJ 202
MISM 661

▼ **FUNCTION 5 - ADMINISTRATION**

▼ **A. Access Control Policies/Administration**

▼ **1. Access Control**

- ▼E - Address access management with staff

HSCJ 202
MISM 661

- ▼E - Address work force about access control software management procedures

HSCJ 202
MISM 661

- ▼E - Address work force about access management procedures

HSCJ 202
MISM 661

- ▼E - Address work force about account management procedures

HSCJ 202
MISM 661

- ▼E - Describe data access

HSCJ 202
MISM 661

- ▼*E - Address access control software management with staff

HSCJ 202
MISM 661

▼ **2. Accounts**

- ▼*E - Address account management with staff

HSCJ 202
MISM 661

▼ **3. Authentication**

- ▼E - Address work force about authentication procedures

HSCJ 202
MISM 661

- ▼*E - Address authentication with staff

HSCJ 202
MISM 661

▼ **5. Biometrics**

- ▼*E - Address biometric access management with staff

HSCJ 202
MISM 661

▼ **7. Custodian**

- ▼*E - Identify information resource custodian

HSCJ 202
MISM 661

▼ **8. Disposition**

- ▼*E - Address disposition procedures with staff

HSCJ 202
MISM 661

▼ **9. Due Care**

- ▼*E - Address questions from users about due care

HSCJ 202
MISM 661

▼ **10. Legal**

- ▼E - Address staff about legal monitoring restrictions

HSCJ 202
MISM 661

- ▼*E - Address staff about legal access restrictions

HSCJ 202
MISM 661

▼ **11. Mode of Operation**

- ▼E - Describe modes of operation

HSCJ 202
MISM 661

- ▼E - Identify the dedicated mode of operation

HSCJ 202
MISM 661

- ▼*E - Define modes of operation

HSCJ 202
HSCJ 315
MISM 661

▼ **12. Monitoring**

- ▼ *E - Outline known means of electronic monitoring

HSCJ 202
MISM 661
MISM 662

▼ **13. Owner**

- ▼ E - Define information ownership

HSCJ 202
MISM 661

- ▼ *E - Identify information resource owner

HSCJ 202
MISM 661

▼ **14. Password**

- ▼ *E - Describe a method to force regular password changes and the limitations of the method

HSCJ 202
MISM 661

▼ **15. Separation of Duties**

- ▼ *E - Describe separation of duties

HSCJ 202
MISM 661

▼ **16. Vendors**

- ▼ *E - Facilitate vendor cooperation

HSCJ 202
ISYS 411
MMBA 640

▼ **17. Audit**

- ▼ *E - Address work force about auditing and logging management procedures

HSCJ 202
MISM 661

▼ **B. Access Control Countermeasures**

▼ **2. Authentication**

- ▼ *E - Address work force about authentication procedures

HSCJ 202
MISM 661

▼ **3. Biometrics**

- ▼ *E - Address biometric access management with staff

HSCJ 202
MISM 661

▼ **4. COMSEC Policy**

- ▼ E - List national COMSEC procedures

HSCJ 202
MISM 661

- ▼ *E - List national COMSEC policies

HSCJ 202
MISM 661

▼ **5. Control**

- ▼*E - Define internal controls and security
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **6. Countermeasures**
 - ▼E - Define countermeasures
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼E - Give examples of countermeasures
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼*E - Describe countermeasures
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **8. Intrusion**
 - ▼E - Address intrusion detection management with staff
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼E - Address staff about intrusion detection
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼E - Address staff about intrusion deterrents
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼*E - Identify methods of intrusion detection
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **9. Isolation and Mediation**
 - ▼*E - Define isolation and mediation
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **10. Key**
 - ▼E - Submit requirements key management
 - [HSCJ 202](#)
 - [HSCJ 315](#)
 - [MISM 661](#)
 - ▼*E - Demonstrate knowledge of how to operate a KMI-enabled system
 - [HSCJ 202](#)
 - [HSCJ 315](#)
 - [MISM 661](#)
- ▼ **11. Monitoring**
 - ▼E - Address staff about monitoring and auditing intrusion detection policies
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼E - Address work force about monitoring management procedures
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼*E - Address monitoring management with staff

HSCJ 202

MISM 661

▼ **12. Network**

- ▼ E - Describe network security software

HSCJ 202

MISM 670

MISM 661

- ▼ *E - Define network firewalls

HSCJ 202

MISM 670

MISM 661

▼ **13. Password**

- ▼ *E - Address password management with staff

HSCJ 202

MISM 661

▼ **C. Access Control Mechanisms**

▼ **1. Access Control**

- ▼ E - Define mandatory access controls

HSCJ 202

MISM 661

- ▼ E - Describe discretionary access controls

HSCJ 202

MISM 661

- ▼ E - Describe mandatory access controls

HSCJ 202

MISM 661

- ▼ *E - Define discretionary access controls

HSCJ 202

MISM 661

▼ **4. Biometrics**

- ▼ *E - Describe biometrics

HSCJ 202

MISM 661

▼ **9. Password**

- ▼ E - Define single sign-on

HSCJ 202

MISM 661

- ▼ E - Describe one-time passwords

HSCJ 202

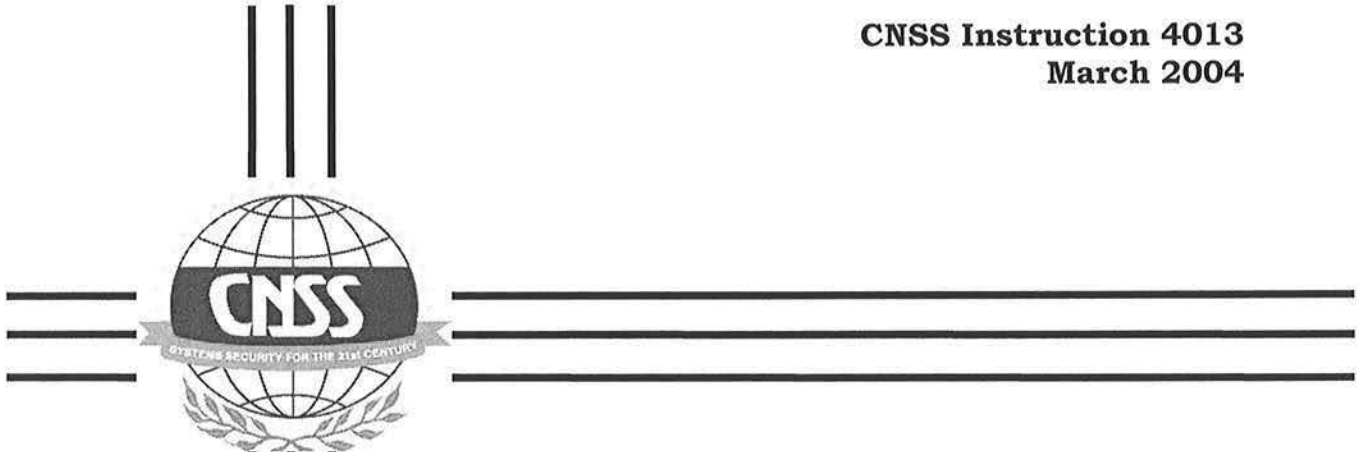
MISM 661

- ▼ *E - Define one-time passwords

HSCJ 202

MISM 661

b. Standard Specifications



NATIONAL INFORMATION
ASSURANCE TRAINING STANDARD
FOR
SYSTEM ADMINISTRATORS (SA)

Awareness, Training and Education (AT&E) are cost-effective methods of improving organizational Information Assurance (IA). In times of ever-contracting budgets, it is difficult to persuade management to spend money on security and training activities that have no direct impact on the organizational bottom line. This paper describes the process used to aid in the systematic development of training to serve as the first line of defense in Information Assurance (IA). In addition, it describes how these materials are applicable to your organizational long-range plans.

This document provides minimum standards for administrators of national security systems. It also may offer guidelines for administrators of unclassified systems. Your department or agency may require a more stringent implementation.

Committee on National Security Systems



NATIONAL MANAGER

FOREWORD

Since the September 11th terrorist attacks against the sovereignty of the United States and its people, both the President and the Congress have redoubled their efforts to underpin the nation's security. The following guidance, reflecting their support, is intended to assist all federal agencies and private sector entities in protecting their information systems. Only through diligence and a well-trained workforce will we be able to adequately defend the nation's vital information resources.

CNSSI No. 4013 is effective upon receipt. It replaces the National Training Standard for System Administrators in Information Systems Security (INFOSEC), dated August 1997, which should be destroyed.

This instruction establishes the minimum course content or standard for the development and implementation of Information Assurance (IA) training for system administrators (SAs). Please check with your agency for applicable implementing documents.

Additional copies of this instruction can be obtained on the CNSS Website www.nstissc.gov or by contacting the office at the address below.

NATIONAL SECURITY AGENCY
CNSS SECRETARIAT
ATTN: I01C STE 6716
FORT GEORGE G. MEADE, MD 20755-6716

/s/

MICHAEL V. HAYDEN
Lieutenant General, USAF

SYSTEM ADMINISTRATOR

NATIONAL INFORMATION ASSURANCE (IA)

TRAINING STANDARD FOR SYSTEM ADMINISTRATORS

	<u>SECTION</u>
PURPOSE	I
APPLICABILITY	II
RESPONSIBILITIES	III

SECTION I – PURPOSE

1. This instruction establishes the minimum training standard for the development and implementation of Information Assurance (IA) training for System Administrators (SAs).

SECTION II – APPLICABILITY

2. The President’s National Strategy to Secure Cyberspace, Feb 03; National Security Telecommunications and Information Systems Security Directive (NSTISSD) No. 501, 16 Nov 92; Department of Defense Directive (DODD) 8000.1, 27 Feb 00; DoDD 8500.1, 24 Oct 02; Department of Defense Instruction (DODI) 8500.2, 6 Feb 03; and DODI 5200.40, 30 Dec 97 establish the requirements for DOD and other federal departments and agencies to implement training programs for IA professionals. As defined in NSTISSD 501, an IA professional is an individual responsible for the security oversight or management of national security systems during phases of the life cycle. Those directives and others are being implemented in a synergistic environment among departments and agencies, which are committed to vigorously satisfying these IA education and training requirements. The following document is a continuation in a series of minimum training and education standards being developed to assist departments and agencies in meeting their responsibilities in these areas (CNSSI [old NSTISSI] Nos. 4011, 4012, 4014, 4015, and 4016). Implementing the training outlined in this document concomitantly with the above NSTISSIs/CNSSIs will fulfill IA training requirements articulated in NIST 800-16, as mandated by 5 C.F.R. Part 930. The definitions for words used in this instruction are derived from the National Information Assurance (IA) Glossary, NSTISSI No. 4009. Many references pertinent to this instruction may be found in ANNEX B.

3. The body of knowledge listed in this instruction was obtained from a variety of sources, *i.e.*, industry, government, and academia. ANNEX A lists the minimal IA

performance standard for a SA. The APPENDIX provides a series of ancillary, platform specific security features and procedures.

4. This instruction is applicable to all departments and agencies of the U.S. Government and their contractors responsible for the development and implementation of IA training for SAs.

SECTION III - RESPONSIBILITIES

5. Heads of U.S. Government departments and agencies shall ensure that SAs (or their equivalents) are trained to the level of proficiency outlined in this instruction, and that such training is provided to those requiring it at the earliest practicable date.

6. The National Manager shall:

- maintain and provide an IA training standard for SAs to U.S. Government departments and agencies
- ensure that appropriate IA training courses for SAs are developed
- assist other U.S. Government departments and agencies in developing and/or conducting IA training activities for SAs as requested
- maintain a national clearinghouse for training and education materials

Enclosures:

Annex A with Appendix

Annex B

ANNEX A

MINIMAL INFORMATION ASSURANCE (IA) PERFORMANCE STANDARD FOR SYSTEM ADMINISTRATORS (SA)

Job Functions

The IA functions of an SA are:

- 1) working closely with the Information Systems Security Officer (ISSO) to ensure the Information System (IS) or network is used securely
- 2) participating in the Information Systems Security incident reporting program
- 3) assisting the ISSO in maintaining configuration control of the systems and applications software
- 4) advising the ISSO of security anomalies or integrity loopholes
- 5) administering, when applicable, user identification or authentication mechanism of the IS or network.

Terminal Objective:

ENTRY LEVEL: Given various scenarios and typical situations containing information systems security issues, the SA will be able to describe and apply the appropriate actions to manage and administer an IS in a secure manner. To be acceptable, the description and application must be in accordance with applicable IA regulations, policies, and guidelines.

INTERMEDIATE LEVEL: Given various scenarios and typical situations containing information systems security issues, the SA will be able to explain and implement the appropriate actions to manage and administer an IS in a secure manner. To be acceptable, the explanation and implementation must be in accordance with applicable IA regulations, policies, and guidelines.

ADVANCED LEVEL: Given various scenarios and typical situations containing information systems security issues, the SA will be able to verify that the appropriate actions are implemented to manage and administer an IS in a secure manner. To be acceptable, verification must be in accordance with applicable IA regulations, policies, and guidelines.

List of performance items under competencies: *

E = entry level

I = intermediate level

A = advanced level

**Note: These levels are linearly hierarchical*

GENERAL BACKGROUND

The following items constitute a basic literacy necessary for a System Administrator to proceed through the course material.

Definitions for Entry Level SAs

Define access control	Define accountability policy
Define accreditation	Define application development control
Define alarms, signals and reports	Define attack actions
Define assurance	Define authentication
Define audit log	Define biometrics
Define automated security tools	Define certification
Define organizational/agency incident response team	Define change control
Define client-server	Define concepts of multilevel security
Define configuration control	Define configuration management
Define continuity planning	Define copyright protection and licensing
Define corrective actions	Define countermeasures
Define disaster recovery	Define documentation
Define EKMS (Electronic Key Management) systems	Define electronic records management
Define error log	Define EMSEC (Emanations Security)/TEMPEST (Short name referring to the investigation, study, and control of compromising emanations from IS equipment) security
Define incident response	Define firewalls
Define information operations	Define information availability
Define integrity	Define information ownership
Define Internet security	Define internal controls
Define KMI systems	Define intrusion

Definitions for Entry Level SAs

Define multilevel security	Define modes of operation
Define one-time passwords	Define object reuse
Define operational procedure review	Define operating system integrity
Define PKI (Public Key Infrastructure) systems	Define password management
Define privacy	Define policy
Define protected distribution systems	Define privileges
Define safeguard	Define privacy
Define security training requirements	Define risk management
Define separation of duties	Define security
Define software piracy	Define sensitive information marking
Define system software controls	Define single sign-on
Define system security architecture study	Define Trusted Network Interpretation
Define validation and testing policies	Define verification and validation process policies
Define zoning and zone of control ratings	

In addition, a Systems Administrator should be able to discuss the following terms before beginning the program of instruction.

Discussion for Intermediate Level SAs

Discuss access authorization	Discuss authentication mechanisms
Discuss client-server security	Discuss configuration management
Discuss continuity plan	Discuss countermeasures
Discuss criminal activity preparedness	Discuss data access
Discuss database integrity	Discuss database security features
Discuss disaster recovery	Discuss documentation
Discuss electronic records management	Discuss privileges
Discuss EMSEC/TEMPEST	Discuss housekeeping procedures
Discuss error log	Discuss security training requirements
Discuss formal approval	Discuss information management
Discuss incident response	Discuss intrusion detection
Discuss information operations	Discuss major operating system security features
Discuss intrusion deterrents	Discuss network security software
Discuss levels of safeguards assurance	Discuss principle elements of security training
Discuss modes of operation	Discuss operating system security features
Discuss object reuse	Discuss privacy

Discussion for Intermediate Level SAs

Discuss objectives of security reviews	Discuss safeguard corrective actions
Discuss policy enforcement	Discuss different levels of countermeasures
Discuss risk management	Discuss objectives of security inspections
Discuss security inspections	

In each of the competency areas listed below, the SA shall perform the following functions at the levels indicated:

FUNCTION ONE – SECURE USE

Working closely with the Information Systems Security Officer (ISSO) to ensure the information systems or network is used securely.

A. General Security Policy

1. Accountability

- E – Define organizational accountability policies
- E – Outline accountability process/program
- I – Discuss organizational accountability policies
- I – Explain organizational accountability policies
- I – Implement organizational accountability policies
- A – Verify implementation of organizational accountability policies

2. Accreditation

- E – Define accreditation
- I – Discuss accreditation
- I – Explain accreditation
- I – Implement accreditation plan/process

3. Architecture

- E – Define system security architecture
- E – Identify appropriate security architecture for use in assigned IS
- E – Address system security architecture study
- I – Discuss system security architecture
- I – Explain system security architecture

4. Assessment

- E – Define assessments for use during certification of information systems
- I – Discuss assessments for use during certification of information systems
- I – Explain assessments for use during certification of information systems
- A – Prepare assessments for use during certification of information systems

5. Assurance

- E – Define assurance
- I – Explain assurance
- I – Discuss assurance

6. Availability/Integrity/Confidentiality/Authentication/Non-repudiation

- E – Define concepts of availability, integrity, confidentiality, authentication, and non-repudiation
- I – Discuss concepts of availability, integrity, confidentiality, authentication, and non-repudiation
- I – Explain concepts of availability, integrity, confidentiality, authentication, and non-repudiation

7. Certification

- E – Define certification policies as related to organizational requirements
- I – Discuss certification policies as related to organizational requirements
- I – Explain certification policies as related to organizational requirements

8. NSTISSP 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA Enabled Information Technology (IT) Products

- E – Identify NSTISSP 11 (Common Criteria) policies
- I – Discuss NSTISSP 11 (Common Criteria) policies
- I – Explain NSTISSP 11 (Common Criteria) policies

9. Configuration Control

- E – Define configuration control (management)
- I – Discuss configuration control (management)
- I – Explain configuration control (management)
- I – Comply with configuration management
- I – Implement configuration control
- I – Maintain configuration control
- A – Verify implementation of configuration control

10. Custodian

- E – Define resource custodian
- E – Identify information resource custodian
- I – Discuss resource custodian

11. Defense in Depth

- E – Define defense in depth
- E – Give examples of defense in depth methods
- E – Give examples of defense in depth policy
- I – Discuss defense in depth
- I – Explain defense in depth

12. Document

- E – Identify DoDD 8500.1 policies (or appropriate civil agency guidance)
- I – Locate DoDD 8500.1 policies (or appropriate civil agency guidance)
- I – Discuss DoDD 8500.1 policies (or appropriate civil agency guidance)
- I – Explain DoDD 8500.1 policies (or appropriate civil agency guidance)

13. Domains

- E – Define security domains as applicable to organizational policies
- E – Describe security domains as applicable to organizational policies
- I – Explain security domains as applicable to organizational policies

14. E-Mail

- E – Define organizational e-mail privacy policies
- I – Discuss organizational e-mail privacy policies
- I – Explain organizational e-mail privacy policies
- I – Implement organizational e-mail privacy policies
- A – Verify implementation of organizational e-mail privacy policies

15. Wireless Security

- E – Identify organizational wireless security policy
- I – Discuss organizational wireless security policy

16. EMSEC/TEMPEST (Emanations Security/Short name referring to the investigation, study, and control of compromising emanations from IS equipment)

- E – Define EMSEC/TEMPEST security policies
- E – Describe EMSEC/TEMPEST control policies
- E – Identify EMSEC/TEMPEST control policies
- E – Identify EMSEC/TEMPEST security policies
- I – Discuss EMSEC/TEMPEST control policies
- I – Discuss EMSEC/TEMPEST security policies
- I – Explain EMSEC/TEMPEST control policies
- I – Explain EMSEC/TEMPEST security policies
- I – Implement EMSEC/TEMPEST control policies
- I – Implement EMSEC/TEMPEST security policies
- A – Verify implementation of EMSEC/TEMPEST control policies
- A – Verify implementation of EMSEC/TEMPEST security policies

17. Ethics

- I – Discuss security policies relating to ethics
- I – Explain security policies relating to ethics

18. FAX

- E – Describe relevant FAX security policies

19. Generally Accepted Security Principles

- E – Define generally accepted systems security principles

- I – Discuss generally accepted systems security principles
- I – Explain generally accepted systems security principles
- A – Comply with generally accepted systems security principles

20. Goals/Mission/Objectives

- E – Define goals, mission, and objectives of the organization
- I – Discuss goals, mission, and objectives of the organization
- I – Explain goals, mission, and objectives of the organization

21. Incident Response

- E – Describe incident response policies
- I – Discuss incident response procedure
- I – Explain incident response policies
- I – Implement incident response policies and procedures

22. Information Assurance

- E – Define organizational Information Assurance (IA) policies
- I – Discuss organizational policies
- I – Explain organizational IA policies
- I – Implement organizational IA policies
- A – Verify implementation of organizational IA policies

23. Information Operations [DOD Organizations Only]

- E – Define information operations
- E – Describe information operations
- E – Support information operations
- I – Explain information operations

24. Internet Security

- E – Describe organizational policies relevant to Internet security

25. Law Enforcement

- E – Identify law enforcement interfaces
- E – Describe law enforcement interfaces
- I – Discuss law enforcement interfaces
- I – Explain law enforcement interfaces

26. Marking

- E – Define policies relating to marking of classified, unclassified and sensitive information
- I – Discuss policies relating to marking of classified, unclassified, and sensitive information
- I – Explain policies relating to marking of classified, unclassified, and sensitive information
- I – Implement policies relating to marking of classified, unclassified, and sensitive information

A – Verify implementation of policies relating to marking of classified, unclassified, and sensitive information

27. Monitoring

- E – Comply with legal aspects of monitoring
- E – Ensure legal aspects of monitoring are enforced

28. Multi-Level Security

- E – Describe multiple secure levels
- E – Identify fundamental concepts of multilevel security
- E – Define fundamental concepts of multilevel security
- E – Describe fundamental concepts of multilevel security
- I – Discuss multiple secure level
- I – Discuss fundamental concepts of multilevel security
- I – Explain fundamental concepts of multilevel security
- I – Explain multiple secure levels
- I – Implement fundamental concepts of multilevel security

29. Network

- E – Describe computer network defense
- E – Describe policies relevant to network security
- E – Describe wide area network (WAN) security policies
- I – Discuss computer network defense
- I – Discuss organizational area network (LAN) security as related to organizational policies
- I – Discuss WAN security policies
- I – Explain computer network defense
- I – Explain organizational area network (LAN) security as related to organizational policies
- I – Explain WAN security policies
- I – Implement WAN security policies
- A – Verify implementation of WAN security policies

30. Operating System

- E – Define functional requirements for operating system integrity
- I – Discuss functional requirements for operating system integrity
- I – Explain functional requirements for operating system integrity
- I – Implement functional requirements for operating system integrity
- A – Verify implementation of functional requirements for operating system integrity

31. Operations Security (OPSEC)

- I – Discuss operations security (OPSEC) in conformance with organizational policies
- I – Explain OPSEC in conformance with organizational policies
- I – Implement OPSEC in conformance with organizational policies
- A – Verify implementation of OPSEC in conformance with organizational policies

32. Ownership

- E – Define information ownership of data held under his/her cognizance
- E – Identify information ownership of data held under his/her cognizance
- E – Identify information resource owner
- I – Discuss information ownership of data held under his/her cognizance
- I – Explain information ownership of data held under his/her cognizance

33. Physical Security

- E – Define physical security
- I – Discuss physical security policies
- I – Explain physical security policies

34. Records Management

- E – Define records management
- E – Describe organizational security policies relative to electronic records management
- I – Discuss records management
- I – Explain records management

35. Secure Systems Operations

- I – Discuss organizational policies relating to secure systems operations

36. Security Policy

- I – Discuss significant agency specific security policies

37. Security Tools

- E – Define automated security tools
- I – Describe automated security tools
- I – Explain automated security tools

38. Sensitivity

- E – Define information sensitivity
- E – Describe information sensitivity in relation to organizational policies
- E – Explain information sensitivity
- I – Discuss information sensitivity

39. Separation of Duties

- E – Define separation of duties
- E – Explain separation of duties
- E – Define organizational policies relating to separation of duties
- I – Discuss organizational policies relating to separation of duties
- I – Explain organizational policies relating to separation of duties
- I – Implement organizational policies relating to separation of duties
- A – Verify implementation of organizational policies relating to separation of duties

40. System Security

- E – Identify systems security standards policies

41. Information Technology Security Evaluation Criteria (ITSEC)

E- Identify Information Security Technology Security Evaluation Criteria (ITSEC) policies

42. Testing

E – Define testing policies

I – Discuss testing policies

I – Explain testing policies

I – Implement testing policies

A – Verify implementation of validation and testing policies

43. Validation/Verification

E – Define validation policies

E – Identify verification and validation process policies

I – Discuss validation policies

I – Discuss verification and validation process policies

I – Explain validation policies

I – Explain verification and validation process policies

I – Implement validation policies

I – Implement verification and validation process policies

A – Verify implementation of validation policies

A – Verify implementation of verification and validation process policies

44. Workstation

E – Describe workstation security policies

I – Discuss workstation security policies

I – Explain workstation security policies

I – Implement workstation security policies

A – Verify implementation of workstation security policies

45. Zone

E – Define zone of control

E – Define zoning

E – Describe zoning and zone of control policies

I – Discuss zoning and zone of control policies

I – Explain zoning and zone of control policies

I – Implement zoning and zone of control policies

A – Verify zoning and zone of control policies

B. General Procedures

1. Network Software

E – Define transport control protocol/internet protocol (TCP/IP)

E – Define transport layer security (*i.e.*, secure socket layer [SSL])

E – Define tunneling protocol (PPTP), layer 2 tunneling protocol (l2tp)

E – Define virtual private network (VPN) (*i.e.*, SSH2, SOCKS)

- E – Describe secure e-mail (*i.e.*, PGP, S/MIME)
- E – Describe secure systems operations procedures
- E – Describe transport control protocol/internet protocol (TCP/IP)
- E – Describe transport layer security (*i.e.*, secure socket layer [SSL])
- E – Describe tunneling protocol (PPTP), layer 2 tunneling protocol (l2tp)
- E – Describe virtual private network (VPN) (*i.e.*, SSH2, SOCKS)
- I – Explain network components (hardware, firmware, software, and media)
- I – Explain secure e-mail (*i.e.*, PGP, S/MIME)
- I – Explain the principles of network security procedures
- I – Explain transport layer security (*i.e.*, secure socket layer [SSL])
- I – Explain tunneling protocol (PPTP), layer 2 tunneling protocol (l2tp)
- I – Explain virtual private network (VPN) (*i.e.*, SSH2, SOCKS)
- I – Implement transport layer security (*i.e.*, secure socket layer [SSL])
- A – Verify implementation of transport layer security (*i.e.*, secure socket layer [SSL])

2. Aggregation

- E – Define aggregation
- E – Describe aggregation
- I – Discuss aggregation
- I – Explain aggregation

3. Application Vulnerabilities

- E – Describe application and system vulnerabilities and threats -- web-based (*i.e.*, XML, SAML)
- E – Describe application and system vulnerabilities and threats -- client-based (*i.e.*, applets, active-X)
- E – Describe application and system vulnerabilities and threats -- server-based
- E – Describe application and system vulnerabilities and threats -- mainframe
- E – Describe application and system vulnerabilities and threats -- malicious code (*i.e.*, Trojan horses, trap doors, viruses, worms)
- I – Explain application and system vulnerabilities and threats -- web-based (*i.e.*, XML, SAML)
- I – Explain application and system vulnerabilities and threats -- client-based (*i.e.*, applets, active-X)
- I – Explain application and system vulnerabilities and threats -- server-based
- I – Explain application and system vulnerabilities and threats -- mainframe
- I – Explain application and system vulnerabilities and threats -- malicious code (*i.e.*, Trojan horses, trap doors, viruses, worms)

4. Architecture

- E – Address system security architecture study
- I – Explain system security architecture study

5. Assessment

- E – Prepare assessments for use during certification of information systems
- I – Explain assessments used during system certification process

6. Automated Tools

- I – Explain expert system tools (*i.e.*, audit reduction and intrusion detection) available
- I – Identify expert system tools (*i.e.*, audit reduction and intrusion detection) available
- I – Use expert system tools (*i.e.*, audit reduction and intrusion detection) available

7. Organizational/Agency Systems Emergency Response Team

- E – Identify organizational/agency systems emergency response team
- E – Report security issues to organizational/agency systems emergency response team
- I – Implement and distribute organizational/agency systems emergency response team reports and advisories
- I – Explain organizational/agency systems emergency response team role

8. Database

- E – Define data mining
- E – Define databases and data warehousing vulnerabilities, threats and protections
- E – Describe data mining
- E – Describe databases and data warehousing vulnerabilities, threats and protections
- I – Explain data mining
- I – Explain databases and data warehousing vulnerabilities, threats and protections

9. EMSEC/TEMPEST

- E – Define EMSEC/TEMPEST security procedures
- E – Identify certified EMSEC/TEMPEST technical authority (CTTA)
- E – Identify EMSEC/TEMPEST security procedures
- I – Discuss EMSEC/TEMPEST security procedures
- I – Explain EMSEC/TEMPEST security procedures

10. End Systems

- E – Define end systems (*i.e.*, workstations, notebooks, PDA [personal digital assistant], smartphones, etc.)
- E – Describe end systems (*i.e.*, workstations, notebooks, PDA, smartphones, etc.)
- I – Explain end systems (*i.e.*, workstations, notebooks, PDA, smartphones, etc.)
- I – Explain threats/vulnerabilities of end systems (*i.e.*, workstations, notebooks, PDA, smartphones, etc.)
- I – Identify threats/vulnerabilities of end systems (*i.e.*, workstations, notebooks, PDA, smartphones, etc.)

11. Facility Management

- E – Practice facility management procedures
- I – Explain importance of sound facility management procedures
- I – Implement facility management procedures
- A – Verify implementation of facility management procedures

12. FAX

- E – Describe FAX security policies/procedures
- E – Practice FAX security policies/procedures

- I – Implement FAX security policies/procedures
- A – Verify implementation of FAX security policies/procedures

13. Housekeeping

- E – Define housekeeping procedures
- E – Describe housekeeping procedures
- E – Perform housekeeping procedures
- I – Explain housekeeping procedures

14. Inference

- E – Define Inference
- E – Describe Inference
- I – Explain Inference

15. Information States

- E – Define information states procedures
- E – Describe information states procedures
- A – Distinguish among information states procedures

16. Internet

- E – Define Internet security procedures
- I – Discuss Internet security procedures
- I – Explain Internet security procedures
- I – Implement Internet security procedures
- A – Verify implementation of Internet security procedures

17. Investigations

- E – Assist in investigations as requested

18. IPSEC

- E – Define IPSEC authentication and confidentiality
- E – Describe IPSEC authentication and confidentiality
- I – Explain IPSEC authentication and confidentiality

19. Marking

- E – Perform marking of sensitive information procedures (defined in C.F.R. 32 Section 2003, National Security Information - Standard Forms) as an example
- I – Discuss marking of sensitive information procedures (defined in C.F.R. 32 Section 2003, National Security Information - Standard Forms) as an example
- I – Explain marking of sensitive information procedures (defined in C.F.R. 32 Section 2003, National Security Information - Standard Forms) as an example
- I – Implement marking of sensitive information procedures (defined in C.F.R. 32 Section 2003, National Security Information - Standard Forms) as an example
- A – Verify implementation of marking of sensitive information procedures (defined in C.F.R. 32 Section 2003, National Security Information – Standard Forms) as an example

20. Multi-Level Security

- E – Define multilevel security
- I – Discuss multilevel security
- I – Explain multilevel security
- I – Apply multilevel security

21. Network, General

- E – Define network architecture/topologies (*i.e.*, ETHERNET, FDDI, bus, star, mesh, etc.)
- E – Define network components (hardware, firmware, software, and media)
- E – Define network layer security
- E – Define network protocols
- E – Define network types
- E – Define wireless security
- E – Describe network architecture/topologies (*i.e.*, ETHERNET, FDDI, bus, star, mesh, etc.)
- E – Describe network components (hardware, firmware, software, and media)
- E – Describe network layer security
- E – Describe network protocols
- E – Describe network types
- E – Describe WAN security procedures
- E – Describe wireless security
- E – Discuss network architecture/topologies (*i.e.*, ETHERNET, FDDI, bus, star, mesh, etc.)
- E – Practice WAN security procedures
- I – Explain network architecture/topologies (*i.e.*, ETHERNET, FDDI, bus, star, mesh, etc.)
- I – Explain network layer security
- I – Explain network types
- I – Explain wireless security
- I – Implement network security procedures
- I – Implement secure data communications
- I – Implement secure voice and facsimile communications
- I – Implement WAN security procedures
- A – Verify implementation of network security procedures
- A – Verify implementation of WAN security procedures

22. Network Hardware

- E – Define cable characteristics (*i.e.*, twisted pair, fiber)
- E – Define concentrators
- E – Define front-end processors, hubs, modems, multiplexers
- E – Define gateways and routers
- E – Define patch panels
- E – Define routers
- E – Define switches

- E – Describe cable characteristics (*i.e.*, twisted pair, fiber)
- E – Describe concentrators
- E – Describe front-end processors, hubs, modems, multiplexers
- E – Describe gateways and routers
- E – Describe patch panels
- E – Describe routers
- E – Describe switches
- E – Identify gateways and routers
- I – Explain cable characteristics (*i.e.*, twisted pair, fiber)
- I – Explain concentrators
- I – Explain front-end processors, hubs, modems, multiplexers
- I – Explain gateways and routers
- I – Explain patch panels
- I – Explain routers
- I – Explain switches
- I – Implement gateways and routers

23. Network Software

- E – Define firewall architecture (*i.e.*, bastion host, DMZ)
- E – Define firewall technology (*i.e.*, packet filtering, data inspection)
- E – Define secure e-mail (*i.e.*, PGP, S/MIME)
- E – Describe firewall architecture (*i.e.*, bastion host, DMZ)
- E – Describe firewall technology (*i.e.*, packet filtering, data inspection)
- E – Describe secure e-mail (*i.e.*, PGP, S/MIME)
- E – Identify firewall architecture (*i.e.*, bastion host, DMZ)
- E – Identify firewall technology (*i.e.*, packet filtering, data inspection)
- E – Identify secure e-mail (*i.e.*, PGP, S/MIME)
- I – Explain firewall architecture (*i.e.*, bastion host, DMZ)
- I – Explain firewall technology (*i.e.*, packet filtering, data inspection)
- I – Explain secure e-mail (*i.e.*, PGP, S/MIME)
- I – Implement firewall architecture (*i.e.*, bastion host, DMZ)
- I – Implement firewall technology (*i.e.*, packet filtering, data inspection)
- I – Implement secure e-mail (*i.e.*, PGP, S/MIME)

24. Objects

- E – Define object reuse
- E – Define polyinstantiation
- E – Describe object reuse
- E – Describe polyinstantiation
- I – Explain object reuse
- I – Explain polyinstantiation

25. Operating System

- E – Define operating systems security procedures
- E – Describe operating system integrity procedures
- E – Perform operating systems security procedures

- I – Explain operating systems security procedures
- I – Implement operating systems security procedures
- A – Verify implementation of operating systems security procedures

26. OSI (Open Systems Interconnect)

- E – Define application layer security protocols (*i.e.*, secure electronic transactions, secure hypertext, secure remote procedure call)
- E – Define data link layer security
- E – Define network layer security
- E – Define OSI model
- E – Define transport control protocol/ internet protocol (TCP/IP)
- E – Define transport layer security (*i.e.*, secure socket layer [SSL])
- E – Define tunneling protocol (PPTP), layer 2 tunneling protocol (l2tp)
- E – Describe application layer security protocols (*i.e.*, secure electronic transactions, secure hypertext, secure remote procedure call)
- E – Describe data link layer security
- E – Describe network layer security
- E – Describe OSI model
- E – Describe presentation layer
- E – Describe session layer
- E – Describe physical layer
- E – Describe transport control protocol/ internet protocol (TCP/IP)
- E – Describe transport layer security (*i.e.*, secure socket layer [SSL])
- I – Explain application layer security protocols (*i.e.*, secure electronic transactions, secure hypertext, secure remote procedure call)
- I – Explain data link layer security
- I – Explain network layer security
- I – Explain network protocols
- I – Explain OSI model
- I – Explain transport control protocol/ internet protocol (TCP/IP)
- I – Explain tunneling protocol (PPTP), layer 2 tunneling protocol (l2tp)
- I – Implement application layer security protocols (*i.e.*, secure electronic transactions, secure hypertext, secure remote procedure call)
- I – Implement data link layer security
- I – Implement network layer security
- I – Implement transport layer security (*i.e.*, secure socket layer [SSL])

27. Rainbow Series*

- E – Describe purpose and contents of National Computer Security Center TG-005, Trusted Network Interpretation (TNI) or Red Book as examples

*N.B. Given that many have been trained using the Rainbow Series and given the historical context of Rainbow Series data, this body of information remains invaluable in lieu of a more current, national-level body of guidance. See below.

28. NSTISSAM COMPUSEC/1-99

E – Describe purpose and contents of NSTISSAM COMPUSEC/1-99, Advisory Memorandum on the Transition from the Trusted Computer System Evaluation Criteria to the International Common Criteria for Information Technology Security Evaluation

29. Security Procedures

E – Define organizational security procedures

E – Assist in organizational security procedures

30. Security tools

E – Define automated security tools

E – Describe automated security tools

I – Explain automated security tools

31. Vulnerability and Threat

E – Address application and system vulnerabilities and threats -- mainframe

E – Address application and system vulnerabilities and threats -- web-based (*i.e.*, XML, SAML)

E – Address application and system vulnerabilities and threats -- client-based (*i.e.*, applets, active-X)

E – Address application and system vulnerabilities and threats -- server-based

E – Address application and system vulnerabilities and threats -- malicious code (*i.e.*, Trojan Horses, trap doors, viruses, worms)

E – Define application and system vulnerabilities and threats -- web-based (*i.e.*, XML, SAML)

E – Define application and system vulnerabilities and threats -- client-based (*i.e.*, applets, active-X)

E – Define application and system vulnerabilities and threats -- server-based

E – Define application and system vulnerabilities and threats -- mainframe

E – Define application and system vulnerabilities and threats -- malicious code (*i.e.*, Trojan Horses, trap doors, viruses, worms)

E – Describe application and system vulnerabilities and threats -- web-based (*i.e.*, XML, SAML)

E – Describe application and system vulnerabilities and threats -- client-based (*i.e.*, applets, active-X)

E – Describe application and system vulnerabilities and threats -- server-based

E – Describe application and system vulnerabilities and threats -- mainframe

E – Describe application and system vulnerabilities and threats -- malicious code (*i.e.*, Trojan Horses, trap doors, viruses, worms)

I – Explain application and system vulnerabilities and threats -- web-based (*i.e.*, XML, SAML)

I – Explain application and system vulnerabilities and threats -- client-based (*i.e.*, applets, active-X)

I – Explain application and system vulnerabilities and threats -- server-based

- I – Explain application and system vulnerabilities and threats -- mainframe
- I – Explain application and system vulnerabilities and threats -- malicious code (*i.e.*, Trojan Horses, trap doors, viruses, worms)

32. Zone

- I – Explain zoning and zone of control procedures

C. General Awareness, Training and Education (AT&E)

Awareness, Training and Education (AT&E)

- E – Describe attack actions as training issues
- E – Identify sources of AT&E materials
- I – Discuss the objectives of security inspections as a training issue
- I – Discuss the objectives of security reviews as a training issue
- I – Discuss the principle elements of security training
- I – Distinguish among education, training, literacy and awareness
- I – Explain attack actions addressed in training
- I – Explain threat in its application to education, training, and awareness
- I – Give examples of security awareness
- I – Give examples of security training
- I – Implement awareness materials as part of job
- A – Verify implementation of awareness materials as part of job

D. General Countermeasures and Safeguards

1. Assessment

- I – Prepare assessments for use during certification of information systems
- I – Evaluate assessments used during certification of information systems

2. AT&E

- E – Recognize awareness, training, and education (AT&E) as a countermeasure
- I – Implement AT&E as a countermeasure

3. Backup

- E – Define backup critical information
- I – Identify critical information
- I – Discuss backup critical information
- I – Explain backup critical information

4. COMSEC

- E – Identify national COMSEC manager (Custodian)
- E – Identify organizational COMSEC manager (Custodian)
- E – List national COMSEC policies
- E – List national COMSEC procedures
- I – Explain SA COMSEC procedures

5. Countermeasures

- E – Describe what is meant by countermeasures
- I – Discuss different levels of countermeasures assurance
- I – Select countermeasures

6. Digest

- E – Define message digests (*i.e.*, MD5, SHA, HMAC)
- I – Discuss message digests (*i.e.*, MD5, SHA, HMAC)
- I – Explain message digests (*i.e.*, MD5, SHA, HMAC)

7. Digital Signature

- E – Define digital signatures
- I – Discuss digital signatures
- I – Explain digital signatures

8. Due Care

- E – Define due care (due diligence)
- I – Discuss due care (due diligence)
- I – Explain due care (due diligence)

9. E-Mail

- E – Describe e-mail privacy countermeasures
- E – Describe e-mail privacy safeguards
- I – Implement email security (*i.e.*, PGP, PEM)
- I – Operate email security (*i.e.*, PGP, PEM)

10. EMSEC/TEMPEST

- E – Define EMSEC/TEMPEST security countermeasures
- E – Define EMSEC/TEMPEST security safeguards
- I – Explain EMSEC/TEMPEST security countermeasures
- I – Explain EMSEC/TEMPEST security safeguards
- I – Implement EMSEC/TEMPEST security countermeasures
- I – Implement EMSEC/TEMPEST security safeguards

11. Facilities

- E – Define facility support systems (*i.e.*, fire protection and HVAC)
- I – Discuss facility support systems (*i.e.*, fire protection and HVAC)
- I – Explain Facility support systems (*i.e.*, fire protection and HVAC)
- I – Implement Facility support systems (*i.e.*, fire protection and HVAC)
- I – Operate facility support systems (*i.e.*, fire protection and HVAC)

12. Hardware

- E – Define computing and telecommunications hardware/software
- I – Discuss computing and telecommunications hardware/software
- I – Explain computing and telecommunications hardware/software

13. Internet

- E – Define internet security
- I – Explain internet security
- I – Implement internet security

14. Key

- E – Define key creation/distribution
- E – Define key recovery
- E – Define key storage/destruction
- E – Define PKI (Public Key Infrastructure) requirements
- E – Submit requirements for key management within the system
- I – Explain public key infrastructure (PKI) (*i.e.* certification authorities, etc)

15. Legal

- E – Define legal requirements
- I – Discuss legal requirements
- I – Explain Legal requirements

16. Marking

- E – Define marking, handling, storing, and destroying of classified, unclassified, and sensitive information & media
- I – Discuss marking, handling, storing, and destroying of classified, unclassified, and sensitive information & media
- I – Explain marking, handling, storing, and destroying of classified, unclassified, and sensitive information & media
- I – Implement marking, handling, storing, and destroying of classified, unclassified, and sensitive information & media

17. Media

- E – Define magnetic media degaussing
- E – Define marking, handling, storing, and destroying of sensitive information & media
- E – Define media (*i.e.*, tape, paper or disks) management
- E – Define secure data deletion for media reuse
- I – Discuss magnetic media degaussing as an example of destruction
- I – Discuss marking, handling, storing, and destroying of sensitive information & media
- I – Discuss media (*i.e.*, tape, paper or disks) management
- I – Discuss secure data deletion for media reuse
- I – Explain magnetic media degaussing as an example of destruction
- I – Explain marking, handling, storing, and destroying of sensitive information & media
- I – Explain media (*i.e.*, tape, paper or disks) management
- I – Explain secure data deletion for media reuse
- I – Implement magnetic media degaussing as an example of destruction
- I – Implement marking, handling, storing, and destroying of sensitive information & media
- I – Implement secure data deletion for media reuse

18. Misuse

- E – Define resource misuse prevention
- I – Discuss resource misuse prevention
- I – Explain resource misuse prevention
- I – Implement resource misuse prevention

19. Non-Repudiation

- E – Define digital non-repudiation
- I – Discuss digital non-repudiation
- I – Explain digital non-repudiation

20. Operations

- E – Describe information operations
- I – Discuss information operations

21. Privacy

- E – Define privacy and protection
- I – Discuss privacy and protection
- I – Explain privacy and protection
- I – Implement privacy and protection

22. Privilege

- E – Define need-to-know/least privilege
- E – Define operator/administrator privileges
- I – Discuss need-to-know/least privilege
- I – Discuss operator/administrator privileges
- I – Explain need-to-know/least privilege
- I – Explain operator/administrator privileges
- I – Implement need-to-know/least privilege
- I – Implement operator/administrator privileges

23. Record

- E – Define record retention
- I – Discuss record retention
- I – Explain record retention
- I – Implement record retention

24. Safeguards

- E – Define safeguards used to prevent software piracy
- E – Describe what is meant by safeguards
- I – Discuss different levels of safeguards assurance

25. Separation of Duties

- E – Describe separation of duties as a countermeasure
- E – Explain separation of duties as a countermeasure
- I – Discuss separation of duties as a countermeasure

26. Software Countermeasure

- E – Define anti-virus systems
- E – Define countermeasures used to prevent software piracy
- I – Discuss anti-virus management
- I – Discuss computing and telecommunications hardware/ software
- I – Explain anti-virus management
- I – Explain computing and telecommunications hardware/ software
- I – Implement anti-virus management
- I – Use anti-virus tools and procedures

27. Testing

- E – Identify automated tools for security testing
- I – Implement automated tools for security testing
- A – Evaluate automated tools for security testing

28. Tools

- E – Describe automated tools for security compliance
- E – Describe automated tools for security test
- I – Implement automated security tools
- I – Implement automated tool for security test
- I – Implement automated tools for security compliance
- I – Operate automated security tools
- I – Operate automated tool for security test
- I – Operate automated tools for security compliance
- A – Choose automated security tools

29. Zone

- I – Explain what is meant by zoning and zone of control

E. Administrative Countermeasures/Safeguards

1. Alarm

- E – Describe alarms, signals and reports
- E – Identify alarms, signals and reports
- E – Implement alarms, signals and reports

2. Assessment

- E – Assist in preparing assessments
- E – Prepare assessments for use during certification of information systems

3. System Test and Evaluation (ST&E)

- E – Discuss System Test and Evaluation (ST&E) Plan and Procedures
- E – Recommend revisions to System Test and Evaluation (ST&E) Plan and Procedures

4. Audit

- E – Identify audit collection requirements
- I – Enforce audit collection requirements
- I – Implement audit trails and logging policies
- A – Verify implementation of audit trails and logging policies

5. Certification

- E – Discuss certification tools
- E – Identify certification tools
- E – Recommend use of specific certification tools

6. Control

- E – Define application development control
- E – Define system software controls
- E – Differentiate security-related changes from non-security-related changes
- E – Identify storage media protection and control
- I – Implement change controls

7. Countermeasures

- E – Identify countermeasures

8. Disposition

- I – Discuss disposition of classified information
- I – Implement disposition of media and data
- I – Practice disposition of media and data
- I – Use disposition of media and data
- A – Verify implementation of disposition of media and data

9. Intrusion

- I – Discuss intrusion detection resources and policies
- I – Implement intrusion detection policies
- I – Use intrusion detection resources
- A – Verify implementation of intrusion detection resources and policies

10. Key

- I – Implement key management techniques
- I – Use key management techniques

11. Labeling

- I – Implement document labeling
- I – Practice document labeling
- I – Use document labeling
- A – Verify implementation of document labeling

12. Password

- E – Address password management with staff

- E – Identify password management systems
- E – Define password management

13. Privacy

- I – Discuss privacy act provisions
- I – Explain privacy act provisions
- I – Implement privacy act provisions

14. Recovery

- E – Address recovery procedures with staff
- E – Describe disaster recovery procedures
- I – Explain disaster recovery procedures
- I – Implement disaster recovery procedures
- A – Verify implementation of disaster recovery procedures

15. Safeguards

- I – Discuss proper use of security safeguards

16. Separation of Duties

- E – Define separation of duties
- E – Evaluate separation of duties
- E – Implement separation of duties

F. Operations Policies/Procedures

1. Assessment

- E – Support assessments for use during certification of information systems

2. Countermeasures

- E – Identify protective technologies
- E – List protective technologies

3. Crime

- E – Support anti-criminal activity preparedness planning (law enforcement)
- I – Discuss anti-criminal activity preparedness planning (law enforcement)

4. Database

- I – Explain database security features
- I – Implement database security features
- I – Maintain database security features
- I – Use database security features
- A – Verify implementation of database security features

5. Disposition

- E – Identify disposition of media and data policies and procedures
- I – Explain disposition of media and data policies and procedures
- I – Implement disposition of media and data policies and procedures

- I – Perform disposition of media and data policies and procedures
- A – Verify implementation of disposition of media and data policies and procedures

6. Documentation

- E – Describe documentation policy and procedures
- I – Implement documentation policy and procedures
- I – Use documentation policy and procedures
- A – Verify implementation of documentation policy and procedures

7. Media

- E – Identify storage media control policies and procedures
- E – Identify storage media protection policies and procedures

8. Objects

- I – Discuss object reuse policy and procedures
- I – Implement object reuse policy and procedures

9. Privacy

- E – Outline known means of keystroke monitoring

10. Recovery

- E – Define disaster recovery policies and procedures
- E – Describe disaster recovery policies and procedures
- I – Implement disaster recovery policies and procedures
- I – Use disaster recovery policies and procedures
- A – Verify implementation of disaster recovery policies and procedures

11. Separation of Duties

- E – Describe separation of duties policies and procedures
- I – Implement separation of duties policies and procedures
- I – Practice separation of duties policies and procedures
- I – Use separation of duties policies and procedures
- A – Verify implementation of separation of duties policies and procedures

12. Vendor

- E – Facilitate vendor cooperation
- E – Explain vendor cooperation

G. Contingency/Continuity of Operations

1. Backup

- E – Outline security policy for backup procedures
- I – Develop security policy for backup procedures

2. Certification

- I – Prepare assessments for use during certification of information systems

3. Continuity/Contingency

- E – Describe continuity/contingency planning
- E – Prepare input to continuity/contingency plan
- I – Discuss continuity/contingency plan
- I – Exercise continuity/contingency plan
- I – Implement continuity/contingency plan
- A – Verify implementation of continuity/contingency plan
- A – Write continuity/contingency plan
- A – Test continuity/contingency plan
- A – Evaluate continuity/contingency plan testing results

4. Recovery

- E – Describe disaster recovery
- E – Describe disaster recovery plan testing
- E – Prepare input to recovery plan
- I – Discuss disaster recovery planning
- I – Exercise disaster recovery operations
- I – Implement disaster recovery
- I – Implement disaster recovery plan testing
- I – Implement disaster recovery planning
- I – Perform contingency operations
- I – Perform disaster recovery
- I – Perform disaster recovery planning
- A – Verify implementation of disaster recovery plans, policies, and procedures
- A – Verify implementation of disaster recovery plan testing
- A – Verify implementation of disaster recovery planning
- A – Evaluate disaster recovery plan exercise results
- A – Write recovery plan
- A – Include lessons-learned from disaster recovery test in new disaster recovery plan

FUNCTION 2 – INCIDENTS

Participating in the Information Systems Security incident reporting program

A. Policy and Procedures

1. Attack

- I – Identify attack
- I – Identify appropriate attack response
- I – Implement attack response

2. Disposition

- E – Address disposition procedures with staff

3. Due Care

- E – Address questions from users about due care

4. Incident

- E – Define incidents
- E – Define breaches
- E – Address unauthorized access incident reporting with staff
- E – Define incident response
- I – Discuss breaches
- I – Discuss incident response
- I – Discuss incidents
- I – Enforce incident response policy/procedures
- I – Explain incident response
- I – Implement incident response
- I – Implement incident response policy/procedures
- A – Verify implementation of incident response policy/procedures are implemented
- I – Discuss evidence preservation
- I – Implement evidence preservation IAW legal guidance

5. Intrusion

- E – Define intrusion detection
- E – Address intrusion detection management with staff
- I – Discuss intrusion detection
- I – Implement intrusion detection
- A – Verify implementation of intrusion detection is implemented

6. Legal

- E – Assist appropriate authority in witness interviewing/interrogation
- E – Assist in evidence identification/preservation

7. Reporting

- E – Define reporting
- I – Discuss reporting
- I – Explain reporting

8. Response

- I – Discuss attacks response

9. Violation

- E – Define violations
- I – Discuss violations
- I – Explain violations

B. Operations Countermeasures/Safeguard

1. Alarm

- I – Use alarms, signals, and reports

2. Attack

- E – Identify an attack
- A – Analyze an attack
- A – Summarize an attack

3. Audit

- I – Implement audit trails and logging policies
- A – Verify implementation of audit trails and logging policies

4. Authentication

- E – Address work force about authentication procedures
- I – Implement authentication policies and procedures
- A – Verify implementation of authentication policies and procedures

5. Organizational/Agency Systems Emergency Response Team

- E – Describe the organizational/agency systems emergency/incident response team
- I – Use the organizational/agency systems emergency/incident response team
- I – Comply with procedures of the organizational/agency systems emergency/incident response team

6. Countermeasure

- E – Assist in performing countermeasure/safeguard corrective actions
- E – Describe countermeasures
- I – Discuss countermeasure
- I – Implement countermeasures
- I – Use countermeasures
- A – Perform countermeasures
- A – Verify implementation of countermeasures

7. Incident

- E – Address unauthorized access incident reporting with staff
- E – Assist in incident response
- I – Implement incident response
- I – Report incident response
- A – Perform incident response
- A – Verify implementation of incident response

8. Intrusion

- I – Implement intrusion detection
- I – Monitor intrusion detection
- I – Report intrusion
- A – Perform intrusion detection
- A – Verify implementation of intrusion detection
- A – Verify implementation of intrusion detection posture

9. Legal

- E – Assist appropriate authority in witness interviewing/interrogation

10. Safeguard

- E – Describe safeguards
- I – Discuss safeguard corrective actions
- I – Implement safeguards
- I – Use safeguards
- A – Verify implementation of safeguards

C. Contingency Countermeasures/Safeguards

1. Alarms

- I – Use alarms, signals, and reports

2. Availability

- E – Define information availability

3. Correction

- E – Identify examples of corrective actions

4. Countermeasures

- I – Select countermeasures with ISSO

5. Incident

- E – Address unauthorized access incident reporting with staff

6. Intrusion

- E – Identify methods of intrusion detection

7. Safeguards

I – Select appropriate safeguards with ISSO

FUNCTION 3 -- CONFIGURATION

Assist the ISSO in maintaining configuration control of the systems and applications software.

Administrative Policies/Procedures

1. Access

I – Discuss access authorization
I – Implement access authorization
A – Verify implementation of access authorization

2. Approval To Operate (ATO)

I – Discuss formal approval to operate
I – Implement formal approval
A – Verify implementation of formal approval to operate

3. Authentication

E – Address authentication with staff
E – Address work force about authentication procedures

4. Biometrics

E – Address biometric access management with staff

5. Organizational/Agency Systems Emergency/Incident Response Team

E – Identify organizational/agency systems emergency/incident response team
I – Implement organizational/agency systems emergency/incident response team security reporting

6. Configure

E – Define change control policies
E – Define configuration control
E – Address configuration management with staff
E – Address staff about legal configuration restrictions
E – Adhere to configuration control
E – Monitor configuration control
I – Implement change control policies
I – Implement configuration control
I – Maintain configuration control
A – Verify implementation of change control policies

7. Copyright

- E – Adhere to copyright protection and licensing
- E – Define copyright protection and licensing
- I – Implement copyright protection and licensing
- A – Verify implementation of copyright protection and licensing

8. Documentation

- I – Discuss documentation
- I – Implement documentation
- A – Verify implementation of documentation

9. Inspection

- I – Discuss security inspections
- I – Implement security inspections
- A – Verify implementation of security inspection report recommendations

10. Install/Patch

- E – Identify appropriate sources for updates and patches
- I – Describe how to install multiple patches with a single batch file
- I – Implement and manually install a patch from an appropriate source
- I – Implement and verify a security patch or upgrade
- I – Implement multiple patches with a single batch file
- I – Implement operating system from appropriate source
- A – Verify and manually install a patch from an appropriate source
- A – Verify implementation of a security patch or upgrade
- A – Verify implementation of multiple patches with a single batch file
- A – Verify implementation of operating system from appropriate source

11. Logging

- I – Describe the different categories of activities which may be logged

12. Management

- E – Identify basic/generic management issues

13. Network

- I – Explain network security software
- I – Implement network security software
- A – Verify implementation of network security software

14. Objects

- I – Describe object reuse

15. Operation

- E – Define operational procedure review
- I – Implement operational procedure review
- A – Verify implementation of operational procedure review

16. Password

- E – Address password management with staff
- I – Describe organizational password management policy

17. Policy

- I – Discuss policy enforcement
- I – Implement policy enforcement
- A – Verify implementation of policy enforcement

18. Records

- I – Explain electronic records management
- I – Implement electronic records management
- A – Verify implementation of electronic records management

19. Wireless

- I – Describe organizational wireless use policy

FUNCTION 4 – ANOMALIES AND INTEGRITY

Advise the ISSO of security anomalies or integrity loopholes.

A. General Risk Management

1. Attack

- E – Describe attack actions
- E – Identify attack actions
- I – Explain attack actions

2. Defense in Depth

- I – Summarize defense in depth

3. EMSEC/TEMPEST

- E – Define EMSEC/TEMPEST security as it relates to the risk management process
- E – Describe EMSEC/TEMPEST security as it relates to the risk management process
- I – Explain EMSEC/TEMPEST security as it relates to the risk management process

4. Internet

- E – Describe ways to provide protection for Internet connections
- I – Explain ways to provide protection for Internet connections

5. Legal

- E – Assist in investigations as requested

6. Logging

- E – Describe the different categories of activities which may be logged

7. Network

- E – Describe wireless security
- E – Describe LAN/WAN security
- I – Explain wireless security
- I – Explain LAN/WAN security

8. Operating System

- E – Describe operating system integrity

9. Risk

- I – Report risks to ISSO

10. Threat

- E – Identify different types of threat
- I – Report threats to ISSO

11. Zone

- E – Describe on what zoning and zone of control ratings are based
- I – Explain zoning and zone of control ratings

B. Access Control Safeguards

1. Access Control

- E – Address access control software management with staff
- E – Address work force about access control software management procedures
- E – Define decentralized/distributed -- single sign on (SSO) (*i.e.*, Kerberos)
- E – Define discretionary access controls
- E – Define mandatory access controls
- E – Define security domain
- E – Describe access control physical, logical, and administrative configurations
- E – Describe access rights and permissions
- E – Describe control techniques and policies (*i.e.*, discretionary, mandatory, and rule of least privilege)
- E – Identify access control attacks (brute force, dictionary, spoofing, denial of service, etc.)
- I – Explain access control attacks (brute force, dictionary, spoofing, denial of service, etc.)
- I – Explain access control physical, logical, and administrative configurations
- I – Explain access rights and permissions
- I – Explain control techniques and policies (*i.e.*, discretionary, mandatory, and rule of least privilege decentralized/distributed -- single sign on (SSO) (*i.e.*, Kerberos)
- I – Explain identification and authentication techniques
- I – Explain security domain
- I – Explain single/multifactor authentication (knowledge based *i.e.*, password/pass phrase, one time, tokens/smart cards and characteristic based *i.e.*, biometrics)
- I – Implement access control physical, logical, and administrative configurations

- I – Implement access rights and permissions
- I – Implement control techniques and policies (*i.e.*, discretionary, mandatory, and rule of least privilege)
- I – Implement decentralized/distributed -- single sign on (SSO) (*i.e.*, Kerberos)
- I – Implement security domain
- A – Use security domain
- A – Use decentralized/distributed -- single sign on (SSO) (*i.e.*, Kerberos)
- A – Use remote access protocols (*i.e.*, PPP/CHAP/PAP/EAP)

2. Alarms

- E – Demonstrate the ability to use alarms, signals, and reports
- A – Use alarms, signals, and reports

3. Authentication

- E – Describe centralized/remote authentication access controls
- E – Describe identification and authentication techniques
- E – Identify identification and authentication techniques
- I – Explain centralized/remote authentication access controls
- A – Use centralized/remote authentication access controls
- A – Use single/multifactor authentication (knowledge based *i.e.*, password/pass phrase, one time, tokens/smart cards and characteristic based *i.e.*, biometrics)

4. Distribution System

- E – Define protected distribution systems

5. Intrusion

- I – Explain intrusion detection

6. Legal

- E – Address staff about legal access restrictions
- E – Assist in investigations as requested

7. Monitor

- E – Define accountability and monitoring (*i.e.*, correction, alarms, audit trail)
- E – Describe accountability and monitoring (*i.e.*, correction, alarms, audit trail)
- I – Explain accountability and monitoring (*i.e.*, correction, alarms, audit trail)
- I – Implement accountability and monitoring (*i.e.*, correction, alarms, audit trail)

8. Network

- E – Identify network security software

9. Operating System

- E – Describe operating system security features

10. Ownership

- E – Describe data ownership and custodianship
- I – Explain data ownership and custodianship

I – Implement data ownership and custodianship

11. Safeguards

E – Describe system security safeguards

I – Implement countermeasures to deter/mitigate attack threats (*i.e.*, malicious code, flooding, spamming)

C. Audit Policies and Procedures

1. Address

E – Address access management with staff

2. Alarms

I – Use alarms, signals, and reports in accordance with existing policies and procedures

3. Audit

I – Implement audit trails and logging policies

I – Summarize audit-related documentation

A – Verify implementation of audit trails and logging policies are implemented

4. Legal

E – Address staff about legal access restrictions

E – Assist in investigations as requested

5. Records

I – Discuss electronic records management relative to compliance with organizational policies and procedures

6. Separation of Duties

E – Describe situations in which separation of duties is appropriate or mandatory

D. Audit Countermeasures/Safeguards

1. Audit

I – Describe safeguards gained through use of audit trails

I – Identify countermeasures applicable to audit trail tampering

2. Legal

E – Assist in investigations as requested

E. Audit Tools

1. Audit

E – Define an error/audit log

E – Identify audit tools

E – Describe the major benefit gained through use of audit trails and logging policies

I – Explain capabilities offered by expert audit tools

I – Explain major benefits of auditing

2. Intrusion

E – Identify intrusion detection systems

3. Legal

E – Assist in investigations as requested

4. Operating Systems

E – Describe major operating system security features

5. Tools

I – Explain capabilities offered by expert security tools

F. Operations Management/Oversight

1. Audit

I – Explain error log

I – Use error log

2. Change Control

I – Implement management/oversight change controls

I – Use management/oversight change controls

A – Verify implementation of management/oversight change controls

3. Configuration Management

E – Describe configuration management

4. Integrity

I – Discuss database integrity

I – Discuss information management

I – Identify the key elements of information integrity

5. Legal

E – Assist in investigations as requested

6. Monitoring

E – Address monitoring management with staff

7. Records

I – Discuss electronic records management

I – Discuss electronic records oversight

8. Recovery

E – Describe disaster recovery management

E – Describe disaster recovery oversight

I – Implement disaster recovery management/oversight

- I – Use disaster recovery management/oversight
- A – Verify implementation of disaster recovery management/oversight

9. Risk

- I – Explain risk management
- I - Practice risk management

G. Configuration Management

1. Architecture

- I – Explain how the security architecture is affected by assurance, trust, and confidence countermeasures; covert channels; EMSEC/TEMPEST; maintenance hooks and privileged programs; states attacks (*i.e.*, time of check / time of use); and timing attacks

2. Change Control

- I – Implement change control policies
- A – Interface with configuration control board

3. Disposition

- I – Perform disposition of media and data
- I – Practice disposition of classified info
- I – Practice emergency destruction
- I – Use disposition of classified info
- I – Use emergency destruction

4. Integrity

- I – Explain database integrity

5. Legal

- E – Assist in investigations as requested

6. Media

- E – Identify storage media protection and control procedures

7. Subjects and Objects

- E – Define subjects and objects

8. Platforms

- I – Explain the elements of technical platforms

9. Records

- I – Explain electronic records management
- I – Perform electronic records management

10. Trusted Computer Base (TCB)

- E – Define trusted computer base (TCB) reference monitors and kernels

FUNCTION 5 -- ADMINISTRATION

Administering, when applicable, security mechanisms of an IS or network

A. Access Control Policies/Administration

1. Access Control

- E – Address access control software management with staff
- E – Address access management with staff
- E – Address work force about access control software management procedures
- E – Address work force about access management procedures
- E – Address work force about account management procedures
- E – Describe data access
- I – Explain access control policies
- I – Use network access controls as designed

2. Accounts

- E – Address account management with staff
- I – Perform account deletions

3. Authentication

- E – Address authentication with staff
- E – Address work force about authentication procedures

4. Awareness, Training and Education (AT&E)

- I – Discuss requirements for security awareness, training, and education

5. Biometrics

- E – Address biometric access management with staff

6. Compartments

- I – Implement compartmented/partitioned mode
- I – Explain compartmented/partitioned mode

7. Custodian

- E – Identify information resource custodian

8. Disposition

- E – Address disposition procedures with staff

9. Due Care

- E – Address questions from users about due care

10. Legal

- E – Address staff about legal access restrictions

E – Address staff about legal monitoring restrictions

11. Mode of Operation

- E – Define modes of operation
- E – Describe modes of operation
- E – Identify the dedicated mode of operation
- I – Use modes of operation

12. Monitoring

E – Outline known means of electronic monitoring

13. Owner

- E – Identify information resource owner
- E – Define information ownership

14. Password

E – Describe a method to force regular password changes and the limitations of the method

15. Separation of Duties

E – Describe separation of duties

16. Vendors

E – Facilitate vendor cooperation

17. Audit

E – Address work force about auditing and logging management procedures

B. Access Control Countermeasures

1. Awareness, Training and Education (AT&E)

- I – Develop security training plan and materials for information system users
- I – Discuss security education
- I – Encourage employees to seek education in IA as a countermeasure
- I – Monitor changing security education requirements for information system users

2. Authentication

E – Address work force about authentication procedures

3. Biometrics

E – Address biometric access management with staff

4. COMSEC Policy

- E – List national COMSEC policies
- E – List national COMSEC procedures
- I – Discuss COMSEC procedures

5. Control

- E – Define internal controls and security
- I – Discuss internal controls and security

6. Countermeasures

- E – Describe countermeasures
- E – Define countermeasures
- E – Give examples of countermeasures
- I – Discuss countermeasures

7. Firewalls

- I – Discuss network firewalls

8. Intrusion

- E – Identify methods of intrusion detection
- E – Address intrusion detection management with staff
- E – Address staff about intrusion detection
- E – Address staff about intrusion deterrents

9. Isolation and Mediation

- E – Define isolation and mediation
- I – Discuss isolation and mediation
- I – Implement isolation and mediation
- I – Monitor isolation and mediation

10. Key

- E – Demonstrate knowledge of how to operate a KMI-enabled system
- E – Submit requirements key management

11. Monitoring

- E – Address monitoring management with staff
- E – Address staff about monitoring and auditing intrusion detection policies
- E – Address work force about monitoring management procedures

12. Network

- E – Define network firewalls
- E – Describe network security software

13. Password

- E – Address password management with staff

14. Tools

- I – Operate automated security tools
- I – Operate automated tools for security compliance
- A – Evaluate automated security tools
- A – Evaluate automated tools for security compliance

C. Access Control Mechanisms

1. Access Control

- E – Define discretionary access controls
- E – Define mandatory access controls
- E – Describe discretionary access controls
- E – Describe mandatory access controls
- I – Use access control software
- I – Implement access control software

2. Audit

- I – Use audit trails and logging policies
- I – Implement audit trails and logging policies
- I – Maintain audit trails and logging policies

3. Authentication

- I – Implement authentication mechanisms
- I – Discuss authentication mechanisms

4. Biometrics

- E – Describe biometrics
- I – Implement biometrics
- I – Use biometrics

5. Database

- I – Discuss database security features
- I – Implement database security features

6. Isolation and Mediation

- I – Implement isolation and mediation
- I – Monitor isolation and mediation
- I – Use isolation and mediation

7. Key

- I – Use KMI applications
- I – Use KMI products
- I – Implement KMI applications
- I – Implement KMI products

8. Operating System

- I – Discuss operating system security features
- I – Use operating system security features
- I – Implement operating system security features
- I – Maintain operating system security features

9. Password

- E – Define one-time passwords
- E – Define single sign-on
- E – Describe one-time passwords
- I – Use single sign-on
- I – Implement single sign-on

10. Privilege

- I – Discuss privileges

11. Security

- I – Discuss client-server security
- I – Use client-server security
- I – Use database security features
- I – Implement client-server security
- I – Maintain client-server security

APPENDIX

PLATFORM SPECIFIC SECURITY FEATURES/PROCEDURES

Many platform or organization specific security features/procedures are ephemeral and should be defined by the agency, service, or organization employing the ISSO. The following list of knowledge items, contributed by a consortium of public/private sector interests, has been identified as high-frequency-of-change and is an example of constantly evolving best practices at the moment. Organizations should establish mechanisms to fold these types of items into their training implementations. They should be considered as ancillary to the primary training standard.

Windows Data		
W1	Background Knowledge	
W1.01	K	Define "windows domain".
W1.02	K	Define "domain controller".
W1.03	K	Define "organizational user account".
W1.04	K	Define "domain user account".
W1.05	K	Define "computer account".
W1.06	K	Define "domain member" (or "member server").
W1.07	K	Define "NetBios name".
W1.08	K	Define "CIFS" (a.k.a."SMB")
W1.09	K	Define "shared folder".
W1.10	K	Define "NTFS" and "FAT".
W1.11	K	Define "registry".
W1.12	K	Describe some of the essential differences between the two main families of Microsoft operating systems: Windows 95/98/Me and Windows NT/2000/XP/.NET.
W1.13	K	Be familiar with the following Microsoft program: Active Directory Users and Computers MMC snap-in.
W1.14	K	Be familiar with the following Microsoft program: Certificates MMC snap-in.
W1.15	K	Be familiar with the following Microsoft program: Computer Management MMC snap-in.
W1.16	K	Be familiar with the following Microsoft program: DCPROMO.EXE
W1.17	K	Be familiar with the following Microsoft program: Event Viewer MMC snap-in.
W1.18	K	Be familiar with the following Microsoft program: IP Security Policies MMC snap-in.
W1.19	K	Be familiar with the following Microsoft program: IPCONFIG.EXE
W1.20	K	Be familiar with the following Microsoft program: IPSECCMD.EXE (on Windows XP/.NET)
W1.21	K	Be familiar with the following Microsoft program: IPSECPOL.EXE (on Windows 2000)

Appendix-1

Windows Data

W1.22	K	Be familiar with the following Microsoft program: Microsoft Management Console (MMC.EXE)
W1.23	K	Be familiar with the following Microsoft program: NBTSTAT.EXE
W1.24	K	Be familiar with the following Microsoft program: NET.EXE - for each relevant version of Windows
W1.25	K	Be familiar with the following Microsoft program: Network Monitor (NETMON.EXE)
W1.26	K	Be familiar with the following Microsoft program: REGEDIT.EXE
W1.27	K	Be familiar with the following Microsoft program: REGEDT32.EXE
W1.28	K	Be familiar with the following Microsoft program: SECEDIT.EXE
W1.29	K	Be familiar with the following Microsoft program: Security Configuration and Analysis MMC snap-in.
W1.30	K	Be familiar with the following Microsoft program: Security Templates MMC snap-in.
W1.31	K	Be familiar with the following Microsoft program: Task Manager (TASKMGR.EXE)
W1.32	K	Be familiar with the following Microsoft programs: TRACERT.EXE and compare it with ping -a IP.nu.mb.er
W1.33	K	Be familiar with the following Microsoft program: XCACLS.EXE
W1.34	K	Be familiar with the following non-Microsoft program: L0phtCrack
W1.35	K	Be familiar with the following non-Microsoft program: Legion
W1.36	K	Be familiar with the following non-Microsoft program: Nmap
W1.37	K	Be familiar with the following non-Microsoft program: DumpSec
W1.38	K	Be familiar with the following non-Microsoft program: WinDump
W1.39	K	Be familiar with WinPCap and how to install it
W1.40	K	Be familiar with the following non-Microsoft program: SuperCACLS
W1.41	K	Be familiar with the following Microsoft program: SRVINFO.EXE
W1.42	K	Be familiar with the following Microsoft program: HFNETCHK.EXE
W1.43	K	Be familiar with the following Microsoft program: IISLOCKD.EXE
W1.44	K	Define and contrast LM, NTLM and NTLMv2.
W1.45	S	Install Windows NT
W1.46	K	Describe the key security risks involved in the installation of Windows NT
W1.47	S	Install Windows 2000
W1.48	K	Describe the key security risks involved in the installation of Windows 2000
W1.49	S	Install Windows 98/95/ME
W1.50	K	Describe the key security risks involved in the installation of Windows 98/95/ME
W10		Delegation of Authority
W10.1	K	Describe Organizational Units in Active Directory.
W10.2	K	Define "Active Directory permission".
W10.3	K	Describe how Active Directory permissions on user accounts, computer accounts and Group Policy Objects can Be used to delegate authority over these objects.

Appendix-2

Windows Data		
W10.4	S	Use the Delegation of Authority Wizard to give a group the ability to create, delete and modify the user accounts in an Organizational Unit, including the ability to reset passwords on user accounts in that Organizational Unit.
W10.5	S	Use Group Policy to add a global group to the organizational Administrators group on each computer in an Organizational Unit.
W10.6	S	Use Group Policy to give a global group additional user rights on all the computers in an Organizational Unit.
W11 Automation and Scripting Support		
W11.1	K	Define "logon script".
W11.2	S	Deploy logon scripts for both current and legacy clients.
W11.3	K	Describe the variety of command-line tools and scripts that can be obtained from the Microsoft Resource Kit or managing security.
W11.4	S	Use Group Policy to automatically deploy startup, shutdown, logon and logoff scripts to computers throughout the organization.
W11.5	S	Use the Task Scheduler on organizational or remote systems for automating the execution of scripts or programs for security.
W2 Domains and Trusts		
W2.1	K	Define "Active Directory forest".
W2.2	K	Describe trusts and the security consequences of (not) having trusts.
W2.3	K	Describe Active Directory database synchronization among domains in the forest, <i>i.e.</i> , describe domains and forests as "replication boundaries".
W2.4	K	Describe the security consequences of isolating users/computers in their own separate domain, whether that domain is in the forest or not.
W2.5	S	Install Active Directory on a server using DCPROMO.EXE.
W2.6	S	Configure explicit trust relationships.
W3 Group Policy and Security Templates		
W3.01	K	Define "Group Policy".
W3.02	K	Describe the uses of Group Policy for security.
W3.03	S	Create and edit Group Policy Objects in Active Directory.
W3.04	K	Define "security template" as it pertains to Group Policy.
W3.05	S	Edit a security template using the Security Templates MMC snap-in.
W3.06	K	Describe the Security Configuration and Analysis (SCA) snap-in.
W3.07	K	Describe the SECEDIT.EXE tool.
W3.08	S	Audit the settings of a computer using the SCA snap-in.
W3.09	S	Audit the settings of a computer using SECEDIT.EXE.
W3.10	S	Configure a computer using the SCA snap-in.
W3.11	S	Configure a computer using SECEDIT.EXE.
W4 User Accounts and Account Policies		
W4.01	K	Describe the role of user accounts and groups in the Windows security model, especially with respect to NTFS permissions, user rights, and auditing user behavior.

Appendix-3

Windows Data		
W4.02	S	Create users and groups with the Active Directory Users and Computers snap-in.
W4.03	K	Define "strong password".
W4.04	K	Define "password hash".
W4.05	K	Define "CHAP" and "MSCHAP" password protocols
W4.06	K	Define "password policy".
W4.07	K	Describe the importance of enforcing a strong password policy.
W4.08	S	Configure password policy through Group Policy, including minimum password length, maximum password age, password history length, minimum password age, and password complexity requirements.
W4.09	S	Use a password-cracking tool, such as L0phtCrack, to audit the strength of users' passwords on a regular basis.
W4.10	K	Define "account lockout policy".
W4.11	K	Describe the issues surrounding an account lockout policy.
W4.12	S	Configure account lockout policy through Group Policy, including lockout threshold, lockout duration, and bad password count reset interval.
W5 NTFS, Share and Registry Permissions		
W5.01	K	Define "NTFS file system".
W5.02	K	Describe NTFS permissions (DACLS) and audit settings (SACLs).
W5.03	S	Configure an NTFS permission on a folder or file with Windows Explorer.
W5.04	K	Describe how a user's final, cumulative permissions to a file are calculated, based on that user's various group memberships, when that file is accessed over the network through a shared folder on a volume formatted with NTFS.
W5.05	K	Describe how a user's being the "NTFS owner" of a file/folder affects what that user can do with that file/folder.
W5.06	S	Configure NTFS permissions through Group Policy.
W5.07	S	Convert a FAT file system to NTFS with CONVERT.EXE without destroying data.
W5.08	K	Define "shared folder".
W5.09	K	Describe the share permissions: Read, Change, Full Control, Deny.
W5.10	S	Edit a share permission on a folder with Windows Explorer.
W5.11	K	Define "registry".
W5.12	S	Edit registry keys and values with REGEDT32.EXE and REGEDIT.EXE.
W5.13	S	Edit the permissions on a registry key with REGEDT32.EXE
W5.14	S	Configure the permissions of registry keys through Group Policy.
W6 Patches, Hotfixes and Service Packs		
W6.01	K	Define "service pack".
W6.02	K	Describe the effect and importance of applying the latest service pack for security and describe the risks of patching and the need for change control.
W6.03	S	Install a service pack using the graphical installation tool.
W6.04	S	Install a service pack hands-free with the necessary command-line switches.
W6.05	K	Define "slipstreaming a service pack during OS installation".

Appendix-4

Windows Data		
W6.06	S	Extract and merge the files from a service pack into a folder where the operating system installation files have been copied ("-s" switch).
W6.07	K	Define "patch" (or "hotfix").
W6.08	S	Download and manually install a patch from Microsoft.
W6.09	K	Describe how to install multiple patches with a single batch file.
W6.10	K	Describe the capabilities of the Network Hotfix Checker (HFNETCHK.EXE) from Microsoft and the purpose of each of its command-line switches.
W6.11	S	Use HFNETCHK.EXE to determine which patches have not been applied to organizational or remote systems.
W7 Auditing and Logging		
W7.01	K	Define "audit policy".
W7.02	K	Describe the different categories of activities which may be logged.
W7.03	S	Configure audit policy through Group Policy.
W7.04	K	Describe how to audit access to NTFS folders and files.
W7.05	S	Configure NTFS auditing on a folder or file with Windows Explorer.
W7.06	S	Configure NTFS auditing through Group Policy.
W7.07	S	Use Event Viewer to examine the audit logs on a organizational or remote system.
W7.08	S	Export an event log to a tab- or comma-delimited text file with Event Viewer.
W7.09	S	Import a textual log file into a database, spreadsheet or other tool which permits the consolidation and reconstruction of event log data.
W7.10	S	Filter and examine a consolidated event log to reconstruct the activities of a single user, computer or service.
W7.11	K	Describe the shortcomings of 1) using only Event Viewer for analyzing event logs, and 2) logging only to the organizational machine, <i>i.e.</i> , no syslog service.
W8 Encryption Facilities: EFS and IPSec		
W8.01	K	Define "Encrypting File System (EFS)."
W8.02	S	Encrypt a folder using EFS with Windows Explorer or CIPHER.EXE.
W8.03	K	Define "EFS recovery agent."
W8.04	S	Export and delete the private key of the recovery agent from stand-alone computers.
W8.05	S	Change the recovery agent through Group Policy on computers which are domain members.
W8.06	K	Define "Internet Protocol Security (IPSec)."
W8.07	K	Describe the uses of IPSec for secure communications and Virtual Private Networking.
W8.08	S	Use the IP Security Policy snap-in or IPSECPOL.EXE/IPSECCMD.EXE to configure IPSec settings on a system.
W8.09	S	Use Group Policy to configure IPSec settings on computers automatically.
W8.10	K	Define Kerberos and how it works
W9		Backup and Disaster Recovery
W9.01	K	Define "disaster recovery."
W9.02	K	Describe the importance of multiple backups and off-site storage.

Appendix-5

Windows Data

W9.03	K	Describe the user rights necessary to backup and restore files on NTFS volumes.
W9.04	K	Define "system state", especially with regard to domain controllers.
W9.05	S	Use the Windows Backup program (or similar) to back up files and the system state.
W9.06	K	Describe Safe Mode and the Recovery Console.
W9.07	S	Boot a computer using the Recovery Console.
W9.08	S	Boot a computer into Safe Mode.
W9.09	K	Describe how to boot into Directory Services Restore Mode on a domain controller.
W9.10	K	Define "authoritative restore" as this pertains to domain controllers.
W9.11	S	Perform an authoritative restore of Active Directory on a domain controller.
W9.12	K	Describe the Emergency Repair Disk and its uses.
W9.13	S	Create an Emergency Repair Disk.
W9.14	K	Define "EFS recovery agent private key."
W9.15	K	Describe risks of Emergency Repair temporary directories
W9.16	K	Describe how the private key for the Encrypting File System (EFS) recovery agent certificate can be used to decrypt EFS-encrypted files on users' computers.
W9.17	S	Configure all the computers in a domain to use a different EFS recovery agent certificate using Group Policy.
W9.18	S	Back up the EFS recovery agent's private key using the Certificates MMC snap-in.
W9.19	S	Use REGEDT32.EXE or REGEDIT.EXE to back up and restore registry keys

UNIX Data

UI		Background Knowledge: Terms, Concepts and Tools
U1.01	K	DESCRIBE the Unix process model
U1.02	S	USE standard commands to track Unix processes and an editor to edit files
U1.03	K	DESCRIBE the UNIX file system, including partitioning, swap space, and race conditions
U1.04	K, S	DESCRIBE and PERFORM Basic UNIX commands
U1.05	S	DEMONSTRATE knowledge of standard file directory locations under different flavors of UNIX
U1.06	S	DESCRIBE and UTILIZE the X Windows System (including adding and subtracting processes from the system boot process) and DESCRIBE the security implications of the X Windows System (xhost, .Xauthority files, etc) and how to use SSH for X tunneling
U1.07	S	DESCRIBE and UTILIZE the UNIX editing utility (vi)
U1.08	S	DESCRIBE and PERFORM startup and shutdown, including rc/init scripts and chkconfig
U1.09	K	DESCRIBE the Unix set-UID, set-GID mechanism and discuss the security issues with set-UID scripts
U1.10	K	Explain what capabilities root access allows and why root access must be limited to a few users with strong security skills
U1.11	K	Explain what a buffer overflow is and how it can give root access
U2		Administrative Skills
U2.01	S	DESCRIBE and PERFORM from source installations, including make and makefiles, and configure scripts and their common options
U2.02	S	DESCRIBE and UTILIZE the commands to format, partition, mount, and unmount drives under UNIX

Appendix-6

UNIX Data		
U2.03	S	DESCRIBE and UTILIZE commands that can be used to backup and restore system data (<i>i.e.</i> , tar, dd, cpio, dump, restore)
U2.04	S	DESCRIBE and UTILIZE the commands used to manage users and groups and demonstrate the ability to add, delete and disable (but not delete) user accounts
U2.05	K	DESCRIBE ntp; demonstrate understanding of server strata, drift, and significance of time sync with regard to logfiles
U2.06	S	INSTALL and configure ntp/xntp
U2.07	S	DESCRIBE how to use sudo to manage root access; also describe its shortcomings (<i>i.e.</i> , root shell "escape" sequences in common programs like less and vi)
U2.08	S	SET up a cron job and cron security
U2.09	K	DESCRIBE how to limit user disk space usage with quota, and memory and CPU utilization with ulimit; Also how to limit core files, limit processes on a per user basis, and limit open file descriptors on a per-process basis.
U2.10	K	DESCRIBE techniques for tuning common network kernel parameters for security (increasing the half-open connection queue and reducing the time outs, turning off IP forwarding, disabling ICMP redirects, lowering ARP cache timeouts, etc)
U3 Basic Security		
U3.01	K	DESCRIBE auditing and logging associated with UNIX
U3.02	S	DESCRIBE and UTILIZE UNIX network configuration files and commands and list the boot sequence on your version of UNIX
U3.03	K	DESCRIBE Unix permission bits and umask
U3.04	S	IDENTIFY excessive permissions on filesystem objects
U3.05	S	LOCATE & inventory SUID and SGID files; explain their significance
U3.06	S	RECOVER lost Unix passwords by booting from OS media
U3.07	S	RESET normal users' forgotten Unix passwords; reset the root password using single-user-mode
U3.08	K	DESCRIBE how passwords are cryptographically protected in UNIX; explain shadow password file
U3.09	K	DESCRIBE a method to force regular password changes and the limitations of the method
U3.10	K	DESCRIBE the purpose and potential risks associated with .rhosts and hosts.equiv
U3.11	K	DESCRIBE how to validate the integrity of a (downloaded) file using PGP/GPG signatures and/or md5 checksums
U3.12	K	DESCRIBE Kerberos authentication -- both one-time password authentication (and know what two-factor authentication is) as well as public-key based authentication systems
U3.13	S	CHANGE the hostname and/or IP address of a system manually (without re-installing the OS) after the system has been installed and been in production.
U3.14	K	DESCRIBE how to automate the creation of multiple essentially similar machines via Jumpstart or Kickstart or by "cloning" a machine from backup tapes.
U3.15	K	DESCRIBE how to find the latest complete set of security patches for your version of UNIX
U3.16	S	Download, install and verify a security patch or upgrade
U4 Service-Specific Secure Configuration		
U4.01	S	DESCRIBE how to do basic DNS administration including updating zone files and debugging name resolution issues
U4.02	K	DESCRIBE DNS (BIND) and the secure management of DNS (<i>i.e.</i> chrooting, reverse lookups, changing version ID of the running name server, restricting zone transfers and recursive queries, setting up DNS forwarding)
U4.03	K	SET UP certificates for SSL communications
U4.04	S	CONFIGURE Apache for chroot operation; demonstrate understanding of httpd.conf access control options
U4.05	S	CONFIGURE FTP (wu_ftp or ProFTPD, for example) for secure operation including

Appendix-7

UNIX Data		
		chroot, Anonymous, Guest (Restricted UID), etc., and secure execution (unprivileged group, etc)
U4.06	K	DESCRIBE the inetd.conf and xinetd.conf files to enable/disable services
U4.07	S	SECURELY CONFIGURE the inetd.conf/xinetd.conf file(s)
U4.08	K	DESCRIBE sendmail and how to prevent "spam" relaying; include use of smrsh for executing programs in a restricted environment; list the latest sendmail security features
U4.09	K	DESCRIBE nfs and its security implications
U410	K	DESCRIBE NIS and NIS security challenges
U411	K	DESCRIBE RPC security threats such as portmapper attacks and insecure RPC services such as rpc.cmsd, rpc.ttdbserverd
U412	K/S	DESCRIBE and INSTALL/USE TCP Wrappers program to allow mail filtering
U5 Auditing/Prevention Methods		
U5.01	S	EMPLOY lsof AND/OR netstat to identify files and processes in use
U5.02	S	CONFIGURE logging via central syslog host; explain facilities and severities and how to tune message output for most useful data
U5.03	S	DEMONSTRATE how to close off network syslog access on machines that are not logging servers
U5.04	K	DESCRIBE the key log files on a UNIX system that should be regularly audited
U5.05	S	CONFIGURE swatch/logcheck to monitor logfiles for critical events and send appropriate notifications
U5.06	S	DESCRIBE syslog and explain how the different log levels can be used to enhance security monitoring
U5.07	S	CREATE logon/legal banner messages for all organizational & network access
U5.08	K	DESCRIBE Unix ACL permissions if your version of UNIX allows such control.
U5.09	S	DEMONSTRATE ability to create a forensic-grade image of a Unix system suitable for law-enforcement analysis
U5.10	K/S	DESCRIBE and INSTALL/USE Tripwire
U5.11	S	DEMONSTRATE configuration and enabling of system level accounting
U5.12	S	DEMONSTRATE configuration and enabling of process accounting
U5.13	S	DEMONSTRATE configuration and enabling of Kernel-level auditing
U6 Specific Security Tools		
U6.01	K/S	DESCRIBE and INSTALL/CONFIGURE/USE Crack or John the Ripper
U6.02	K/S	DESCRIBE and INSTALL/CONFIGURE/USE TARA
U6.03	K/S	DESCRIBE and INSTALL/CONFIGURE/USE Sniffit or another sniffer
U6.04	S	DEMONSTRATE the ability to use PGP to send and receive signed and encrypted email
U6.05	S	DEMONSTRATE the ability to install and configure a host-based firewall (IP Tables/Chains under Linux or ipf on other UNIX flavors
U6.06	S	DEMONSTRATE the use of Bastille Linux, YASSP, or TITAN to harden UNIX Linux systems before deployment
U6.07	K/S	DESCRIBE and INSTALL/CONFIGURE/USE TCPDump
U6.08	K/S	DESCRIBE and INSTALL/CONFIGURE/USE Secure Shell
U6.09	K/S	DESCRIBE and INSTALL/CONFIGURE/USE Nessus
U6.10	K/S	DESCRIBE and INSTALL/CONFIGURE/USE NMAP
U6.11	K/S	DESCRIBE and INSTALL/CONFIGURE/USE PortSentry

ANNEX B

REFERENCES

The following references pertain to this Instruction:

1. DODD 8000.1, Management of Information Resources and Information Technology, 27 Feb 02
2. DoDD 8500.1, Information Assurance, 24 Oct 02
3. DoDD 8500.1-M, Information Assurance Manual, (when effective)
4. DoD I 8500.2, Information Assurance (IA) Implementation, 6 Feb 03
5. DODI 5200.40, DITSCAP, 30 Dec 97
6. EO 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, 3 Apr 84
7. E O 13231, Critical Infrastructure Protection in the Information Age, 16 Oct 01
8. FIPS 31, Guidelines for Automatic Data Processing Physical Security and Risk Management, Jun 74
9. FIPS Publication 65, Guideline for Automatic Data Processing Risk Analysis, 1 Aug 3
10. FIPS Publication 87, Guidelines for ADP Contingency Planning, 27 Mar 81
11. FIPS Publication 101, Guideline for Life Cycle Validation, Verification, and Testing of Computer Software, 6 Jun 83
12. FIPS Publication 102, Guideline for Computer Security Certification and Accreditation
13. NCSC TG-005, Trusted Network Interpretation (TNI), 31 Jul 87
14. NCSC-TG-027, Version 1, A Guide To Understanding Information System Security Officer Responsibilities for Automated Information Systems
15. NCSC-TG-029, Version 1, Introduction to Certification and Accreditation
16. NIST SP 800-4, Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials, Mar 92
17. NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, Oct 95
18. NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, Sep 96
19. NIST SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-based Model, Apr 98
20. NIST SP 800-18, Guide for Development of Security Plans for Information Technology Systems, Dec 98
21. NSD 42, National Policy for the Security of National Security Telecommunications and Information Systems, 1 Apr 92

22. NSTISSD 501, National Training Program for Information Systems Security (INFOSEC) Professionals, 16 Nov 92
23. NSTISSI No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP), Apr 00
24. NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, 19 May 2003
25. OMB Circular No. A-123, Management Accountability and Control, 21 Jun 95
26. OMB Circular No. A-130, Revised (Transmittal Memorandum No. 4), Management of Federal Information Resources, 30 Nov 00
27. OMB Memorandum M-00-07, Incorporating and Funding Security in Information Systems Investments, 28 Feb 00
28. OMB Memorandum M-01-08, Guidance on Implementing the Government Information Security Reform Act, 16 Jan 01.
29. OMB Memorandum M-01-24, Reporting Instructions for the Government Information Security Reform Act, 22 Jun 01.
30. OMB Memorandum M-02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones, 17 Oct 01.
31. OPM, 5 Combined Federal Regulation (CFR) Part 930, Training Requirements for the Computer Security Act, 3 Jan 92
32. PL 93-579, 5 U.S.C. 552a, the Privacy Act of 1974 (5 U.S.C. 552a)
33. PL 107-347, E-Government Act of 2002, Title III, Federal Information Security Management Act (FISMA), 17 Dec 02
34. PL 100-235, Computer Security Act of 1987, 8 Jan 88 and as amended by the Computer Security Enhancement Act of 1997, 11 Feb 97
35. PL 100-503, the Computer Matching and Privacy Protection Act
36. PL 104-106, Division E, the Information Technology Management Reform Act (Clinger-Cohen Act) of 1996
37. PL 106-398, Title X, Subtitle G, the Government Information Security Reform Act (GISRA)
38. The President's National Strategy to Secure Cyberspace, Feb 03

E. CNSS Standard NTSTISSU 4014

a. Course Mapping Details

Print	Collapse All	Expand All	Previous Page	Next Page
-----------------------	------------------------------	----------------------------	-------------------------------	---------------------------

Welcome Barbara Ciaramitaro, it is Monday, August 16, 2010 at 03:35:51 PM
You are currently viewing a report for CNSI 4014 sorted by element.

▼ **1. DEVELOP CERTIFICATION AND ACCREDITATION POSTURE**

▼ **A. PLANNING FOR CERTIFICATION AND ACCREDITATION**

▼ **(1) Planning**

- ▼ E - Discuss goals, mission, and objectives of the organization(s)

[HSCJ 202](#)
[MISM 661](#)

- ▼ E - Discuss Information Technology Security Evaluation Criteria (ITSEC)

[HSCJ 202](#)
[MISM 661](#)

- ▼ E - Discuss National Information Assurance Program (NIAP) Validated Products List

[HSCJ 202](#)
[MISM 661](#)

- ▼ E - Discuss the components of information systems evaluation models

[HSCJ 202](#)
[MISM 661](#)

- ▼ E - Discuss the concepts of availability, integrity, confidentiality, authentication, and non-repudiation

[HSCJ 202](#)
[MISM 661](#)

- ▼ E - Discuss the constituent components of the certification and accreditation process

[HSCJ 202](#)
[MISM 661](#)

- ▼ E - Discuss the theoretical concepts of security models - commercial systems models

[HSCJ 202](#)
[MISM 661](#)

- ▼ E - Discuss the theoretical concepts of security models - confidentiality models (e.g., Bell & LaPadula)

[HSCJ 202](#)
[MISM 661](#)

- ▼ E - Discuss the theoretical concepts of security models - information flow models

[HSCJ 202](#)
[MISM 661](#)

- ▼ E - Discuss the theoretical concepts of security models - integrity models (e.g., Biba, Clark and Wilson)

[HSCJ 202](#)
[MISM 661](#)

- ▼ E - Explain Common Criteria (CC)

[HSCJ 202](#)
[MISM 661](#)

- ▼ E - Explain Information Technology Security Evaluation Criteria (ITSEC)

[HSCJ 202](#)
[MISM 661](#)

- ▼ E - Explain International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17799

HSCJ 202

MISM 661

- ▼ E - Explain the Model for Information Assurance: An Integrated Approach (2nd Annual IEEE Systems, Man and Cybernetics Information Assurance Workshop, June 2002)

HSCJ 202

MISM 661

- ▼ *E - Define certification and accreditation

HSCJ 202

MISM 661

▼ (2) Defense in Depth

- ▼ *E - Give examples of defense in depth methods

HSCJ 202

MISM 661

▼ (3) Assets

- ▼ E - Define contracts, agreements, and other obligation policy

HSCJ 202

MISM 661

- ▼ E - Define data owner

HSCJ 202

MISM 661

- ▼ E - Define policy for user roles

HSCJ 202

MISM 661

- ▼ E - Define system owner

HSCJ 202

MISM 661

- ▼ E - Discuss user roles

HSCJ 202

MISM 661

- ▼ E - Identify assets

HSCJ 202

MISM 661

- ▼ E - Identify contracts, agreements, and other obligations

HSCJ 202

MISM 661

- ▼ E - Identify data owner

HSCJ 202

MISM 661

- ▼ E - Identify database structure

HSCJ 202

MISM 610

ISIN 200

MISM 661

- ▼ E - Identify system owner

HSCJ 202

MISM 661

- ▼ E - Identify systems interconnection

HSCJ 202

MISM 661

- ▼ *E - Define assets

HSCJ 202

MISM 661

▼ **(4) Threats**

- ▼ E - Define aggregation

HSCJ 202

MISM 661

- ▼ E - Define social engineering threats

HSCJ 202

MISM 661

- ▼ E - Define technological threats

HSCJ 202

MISM 661

- ▼ E - Define threats from careless/disgruntled employees

HSCJ 202

MISM 661

- ▼ E - Describe adversarial threat

HSCJ 202

MISM 661

- ▼ E - Describe how espionage (industrial/international) can impact security of information systems

HSCJ 202

ISIN 330

MISM 661

- ▼ E - Describe how people can threaten system's security, i.e., intentional and unintentional

HSCJ 202

MISM 661

- ▼ E - Describe how security reviews can be used to identify threats to information systems

HSCJ 202

MISM 661

- ▼ E - Describe threat from electronic emanations

HSCJ 202

MISM 661

- ▼ E - Describe threat from natural sources (fire, flood, earthquake, etc)

HSCJ 202

MISM 661

- ▼ E - Describe types of environmental control (air conditioning, filtered power, etc.) threats

HSCJ 202

MISM 661

- ▼ E - Describe types of intentional human threats to system

- HSCJ 202
MISM 661

▼ E - Describe types of unintentional human threats to system
- HSCJ 202
MISM 661

▼ E - Discuss access control attacks (brute force, dictionary, spoofing, denial of service, etc.)
- HSCJ 202
MISM 661

▼ E - Discuss aggregation
- HSCJ 202
MISM 661

▼ E - Discuss application and system vulnerabilities and threats - client-based (e.g., applets, Active-X)
- HSCJ 202
MISM 661

▼ E - Discuss application and system vulnerabilities and threats - mainframe
- HSCJ 202
MISM 662

▼ E - Discuss application and system vulnerabilities and threats - malicious code (e.g., Trojan Horses, trap doors, viruses, worms)
- HSCJ 202
MISM 661

▼ E - Discuss application and system vulnerabilities and threats - server-based
- HSCJ 202
MISM 661
MISM 662

▼ E - Discuss application and system vulnerabilities and threats - web-based (e.g., XML, SAML)
- HSCJ 202
MISM 661

▼ E - Discuss boundary
- HSCJ 202
MISM 661

▼ E - Discuss data mining
- HSCJ 202
MISM 610
MISM 740
STQM 342
MISM 661

▼ E - Discuss databases and data warehousing vulnerabilities, threats and protections
- HSCJ 202
MISM 610
MISM 740
MISM 661

▼ E - Discuss how the security architecture is affected by assurance and confidence
- HSCJ 202
MISM 661

▼ E - Discuss how the security architecture is affected by countermeasures

HSCJ 202

MISM 661

- ▼ E - Discuss how the security architecture is affected by covert channels

HSCJ 202

MISM 661

- ▼ E - Discuss how the security architecture is affected by emanations

HSCJ 202

MISM 661

- ▼ E - Discuss how the security architecture is affected by maintenance hooks and privileged programs

HSCJ 202

MISM 661

- ▼ E - Discuss how the security architecture is affected by resource misuse prevention

HSCJ 202

MISM 661

- ▼ E - Discuss how the security architecture is affected by states attacks (e.g., time of check/time of use)

HSCJ 202

MISM 661

- ▼ E - Discuss how the security architecture is affected by timing attacks

HSCJ 202

MISM 661

- ▼ E - Discuss inference

HSCJ 202

MISM 610

MISM 661

- ▼ E - Discuss natural disaster impacts on system

HSCJ 202

MISM 661

- ▼ E - Discuss object reuse

HSCJ 202

MISM 610

MISM 661

- ▼ E - Discuss perimeter and building grounds protection issues/systems

HSCJ 202

MISM 661

- ▼ E - Discuss polyinstantiation

HSCJ 202

MISM 610

MISM 661

- ▼ E - Discuss security implications posed by portable devices and components

HSCJ 202

HSCJ 315

MISM 661

- ▼ E - Identify access control attacks (brute force, dictionary, spoofing, denial of service, etc.)

HSCJ 202

MISM 661

- ▼ E - Identify appropriate EMSEC/TEMPEST authorities
 - HSCJ 202
 - MISM 661
- ▼ E - Identify process for evaluating threat
 - HSCJ 202
 - MISM 661
- ▼ E - Identify related disciplines that should contribute to risk analysis
 - HSCJ 202
 - MISM 661
- ▼ *E - Define adversarial threat
 - HSCJ 202
 - MISM 661
- ▼ **(5) Vulnerabilities**
 - ▼ E - Define National Information Assurance Program (NIAP) Validated Products List
 - HSCJ 202
 - MISM 661
 - ▼ E - Define Protection Profiles
 - HSCJ 202
 - MISM 661
 - ▼ E - Define vulnerabilities
 - HSCJ 202
 - MISM 661
 - MISM 662
 - ▼ E - Describe agency policy for access by uncleared individuals and vendors
 - HSCJ 202
 - MISM 661
 - ▼ E - Describe agency policy for redeploying classified systems
 - HSCJ 202
 - MISM 661
 - ▼ E - Describe agency/vendor cooperation/coordination
 - HSCJ 202
 - MISM 661
 - MISM 662
 - ▼ E - Describe technical surveillance vulnerabilities
 - HSCJ 202
 - MISM 661
 - MISM 662
 - ▼ E - Describe vulnerability analysis
 - HSCJ 202
 - MISM 661
 - MISM 662
 - ▼ E - Identify technical surveillance vulnerabilities
 - HSCJ 202
 - MISM 661
 - MISM 662
 - ▼ *E - Assist in performance of vulnerability analysis

HSCJ 202

MISM 661

MISM 662

▼ **(6) Criticality**

- ▼ E - Define attack analysis

HSCJ 202

HSCJ 210

MISM 661

MISM 662

- ▼ E - Define criticality

HSCJ 202

MISM 661

- ▼ *E - Define asset criticality

HSCJ 202

MISM 661

▼ **(7) Risk**

- ▼ E - Discuss risk management concepts

HSCJ 202

MISM 661

- ▼ *E - Define risk (threat and vulnerability pairs together with significance)

HSCJ 202

MISM 661

▼ **(8) Conduct Risk Assessment**

- ▼ E - Define risk assessment

HSCJ 202

MISM 661

- ▼ E - Describe risk assessment process

HSCJ 202

MISM 661

- ▼ E - Describe three states of information

HSCJ 202

MISM 661

- ▼ *E - Define information valuation

HSCJ 202

MISM 661

▼ **(9) Countermeasures**

- ▼ E - Define National Information Assurance Program (NIAP) Validated Products List

HSCJ 202

MISM 661

- ▼ E - Describe how countermeasures can mitigate risk

HSCJ 210

MISM 661

- ▼ E - Discuss application environment and security controls

HSCJ 202

MISM 610

MISM 661

- ▼ E - Discuss audit trails/access logs & intrusion detection applications

- HSCJ 202
MISM 661

▼ E - Discuss badging, and smart/dumb cards
- HSCJ 202
MISM 661

▼ E - Discuss biometric access controls to facility
- HSCJ 202
MISM 661

▼ E - Discuss CCTV requirements/capabilities
- HSCJ 202
MISM 661

▼ E - Discuss escort requirements/visitor control issues
- HSCJ 202
MISM 661

▼ E - Discuss fire detection and suppression issues/systems
- HSCJ 202
MISM 661

▼ E - Discuss firewalls
- HSCJ 202
MISM 661

▼ E - Discuss intrusion detection system (e.g., firewalls, motion detectors, sensors, alarms) requirements/capabilities
- HSCJ 202
MISM 661

▼ E - Discuss keys and locks requirements/capabilities
- HSCJ 202
MISM 661

▼ E - Discuss power and HVAC considerations
- HSCJ 202
MISM 661

▼ E - Discuss restricted areas/work areas security requirements
- HSCJ 202
MISM 661

▼ E - Discuss risk management concepts
- HSCJ 202
MISM 661

▼ E - Discuss security guard requirements
- HSCJ 202
MISM 661

▼ E - Discuss site selection and facility design configuration considerations
- HSCJ 202
MISM 661

▼ E - Discuss turnstiles and mantraps requirements
- HSCJ 202
MISM 661

▼ E - Discuss water, leakage, flooding impact to system

- ▼ E - Identify countermeasures to deter/mitigate attack threats (e.g.; malicious code, flooding, spamming)

HSCJ 202

MISM 661

- ▼ *E - Define countermeasures

HSCJ 202

MISM 661

▼ **(10) Organizational/Agency Systems Emergency/Incident Response Team**

- ▼ E - Identify organizational/agency systems emergency/incident response team

HSCJ 202

HSCJ 210

MISM 661

- ▼ *E - Define organizational/agency systems emergency/incident response team

HSCJ 202

HSCJ 210

MISM 661

▼ **(11) Education, Training, & Awareness (ETA)**

- ▼ E - Discuss ETA as a countermeasure

HSCJ 202

MISM 661

- ▼ *E - List topics for inclusion into education, training, and awareness (ETA) policy

HSCJ 202

MISM 661

▼ **(12) Residual Risk**

- ▼ *E - Define residual risk

HSCJ 202

MISM 661

▼ **(13) Cost/Benefit Analysis**

- ▼ E - Define risk acceptance

HSCJ 202

MISM 661

- ▼ *E - Define cost/benefit analysis

HSCJ 202

MISM 661

▼ **B. CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY (CIA) POLICY**

▼ **(1) Contingency Plans**

- ▼ E - Identify items for which plans must be developed

HSCJ 202

MISM 661

- ▼ E - Prepare input to contingency plan

HSCJ 202

MISM 661

- ▼ E - Write contingency plan

HSCJ 202

MISM 661

- ▼ *E - Define contingency plans

HSCJ 202

MISM 661

▼ **(2) Concept of Operations (CONOP)**

- ▼ *E - Define Concept Of Operations (CONOP)

HSCJ 202
MISM 661

▼ **(3) Continuity Plans**

- ▼ E - Discuss business continuity planning (BCP)

HSCJ 202
MISM 661

- ▼ E - Discuss business organization analysis

HSCJ 202
MISM 661

- ▼ E - Discuss disaster recovery planning (DRP) (recovery planning and strategy)

HSCJ 202
MISM 661

- ▼ E - Discuss project scope development and planning

HSCJ 202
MISM 661

- ▼ E - Discuss resource requirements

HSCJ 202
MISM 661

- ▼ E - Identify items for which plans must be developed

HSCJ 202
MISM 661

- ▼ E - Outline security policy for backup procedures

HSCJ 202
MISM 661

- ▼ E - Prepare input to continuity plan

HSCJ 202
MISM 661

- ▼ E - Write continuity plan

HSCJ 202
MISM 661

- ▼ *E - Define continuity plan

HSCJ 202
MISM 661

▼ **(4) Legal Plan**

- ▼ E - Discuss computer crime and various methods used to commit computer crime

HSCJ 202
MISM 661

- ▼ E - Discuss computer crime laws

HSCJ 202
MISM 661

- ▼ E - Discuss Computer Fraud and Abuse Act

HSCJ 202
MISM 661

- ▼ E - Discuss Copyright Act of 1976

- HSCJ 202
MISM 661

▼ E - Discuss Copyright Protection and License
- HSCJ 202
MISM 661

▼ E - Discuss Electronic Freedom of Information Act
- HSCJ 202
MISM 661

▼ E - Discuss Electronic Records Management and Federal Records Act
- HSCJ 202
MISM 661

▼ E - Discuss Federal Information System Management Act
- HSCJ 202
MISM 661

▼ E - Discuss Federal Managers Financial Integrity Act
- HSCJ 202
HSCJ 317
MISM 661

▼ E - Discuss Federal Property and Administration Service Act
- HSCJ 202
MISM 661

▼ E - Discuss Freedom of Information Act
- HSCJ 202
MISM 661

▼ E - Discuss Government Information Security Reform Act
- HSCJ 202
MISM 661

▼ E - Discuss Government Paperwork Elimination Act
- HSCJ 202
MISM 661

▼ E - Discuss implications of the Privacy Act
- HSCJ 202
MISM 661

▼ E - Discuss import/export laws
- HSCJ 202
MISM 661

▼ E - Discuss incident handling and response
- HSCJ 202
HSCJ 210
MISM 661

▼ E - Discuss information systems security laws
- HSCJ 202
MISM 661

▼ E - Discuss intellectual properties laws
- HSCJ 202
MISM 661

▼ E - Discuss international legal issues which can affect information assurance

HSCJ 202

ISIN 330

MISM 661

- ▼ E - Discuss legal responsibilities of the SSM, viz., CIO, DAA, CTO, etc.

HSCJ 202

MISM 661

- ▼ E - Discuss liability laws

HSCJ 202

MISM 661

- ▼ E - Discuss licensing laws

HSCJ 202

MISM 661

- ▼ E - Discuss Millennium Copyright Act

HSCJ 202

MISM 661

- ▼ E - Discuss National Archives and Records Act

HSCJ 202

MISM 661

- ▼ E - Discuss Privacy Act issues

HSCJ 202

MISM 661

- ▼ E - Discuss requirements of Computer Security Act

HSCJ 202

MISM 661

- ▼ E - Discuss the parameters of investigations

HSCJ 202

HSCJ 210

MISM 661

- ▼ E - Discuss trans-border data flow laws

HSCJ 202

MISM 661

- ▼ E - Discuss USA Patriot Act

HSCJ 202

ISIN 330

MISM 661

- ▼*E - Discuss Clinger-Cohen Act

HSCJ 202

MISM 661

- ▼*E - Discuss evidence collection and handling

HSCJ 202

HSCJ 210

MISM 661

- ▼ **(5) Disposition of Classified Material & Emergency Destruction Policy (EDP)**

- ▼ E - Explain emergency destruction policy (EDP) to those who execute plans

HSCJ 202

MISM 661

- ▼*E - Define disposition of classified material

HSCJ 202

MISM 661

▼ **(6) Identification and Authentication (I&A) Policy**

- ▼ E - Define account management

HSCJ 202

MISM 661

- ▼ E - Define authentication

HSCJ 202

MISM 661

- ▼ E - Define biometrics

HSCJ 202

MISM 661

- ▼ E - Define identification and authentication (I&A)

HSCJ 202

MISM 661

- ▼ E - Define non-repudiation

HSCJ 202

MISM 661

- ▼ E - Define peer-to-peer security

HSCJ 202

MISM 661

- ▼ E - Define unauthorized access

HSCJ 202

MISM 661

- ▼ E - Describe how to choose appropriate passwords, and how/why to protect them

HSCJ 202

MISM 661

- ▼ E - Discuss good passwords/password conventions

HSCJ 202

MISM 661

- ▼ E - Discuss non-repudiation

HSCJ 202

MISM 661

- ▼ E - Explain need for account management

HSCJ 202

MISM 661

- ▼ E - List underlying account management principles

HSCJ 202

MISM 661

- ▼ E - List underlying authentication principles

HSCJ 202

MISM 661

- ▼ E - List underlying security concerns with password sharing

HSCJ 202

MISM 661

- ▼ *E - Discuss authentication

HSCJ 202

MISM 661

▼ **(7) Monitoring and Auditing Policy**

- ▼ E - Define intrusion detections
 - HSCJ 202
 - MISM 661
- ▼ E - Define keystroke monitoring
 - HSCJ 202
 - MISM 661
- ▼ E - Define keystroke monitoring requirements for policy and procedures
 - HSCJ 202
 - MISM 661
- ▼ E - Define monitoring
 - HSCJ 202
 - MISM 661
- ▼ E - Define required audit features
 - HSCJ 202
 - MISM 661
- ▼ E - Define requirements for error logs/system logs
 - HSCJ 202
 - MISM 661
- ▼ E - Describe audit collection requirements
 - HSCJ 202
 - MISM 661
- ▼ E - Describe policy for audit
 - HSCJ 202
 - MISM 661
- ▼ E - Identify audit and log tools
 - HSCJ 202
 - MISM 661
- ▼ E - Identify error and system tools
 - HSCJ 202
 - MISM 661
- ▼ E - Outline known means of electronic monitoring
 - HSCJ 202
 - MISM 661
- ▼ E - Outline known means of keystroke monitoring
 - HSCJ 202
 - MISM 661
- ▼ *E - Define electronic monitoring
 - HSCJ 202
 - MISM 661

▼ **C. CONTROL SYSTEMS POLICIES**

▼ **(1) Configuration Management Policy**

- ▼ E - Define Configuration Control Board (CCB)
 - HSCJ 202
 - MISM 661
- ▼ *E - Define configuration management

HSCJ 202

MISM 661

▼ **(2) Protective Technology Policy**

- ▼ E - List protective technologies

HSCJ 202

MISM 661

- ▼ *E - Define protective technology

HSCJ 202

MISM 661

▼ **(3) Intrusion Detection Policy**

- ▼ *E - Define intrusion detection

HSCJ 202

MISM 661

▼ **(4) Malicious Code Policy**

- ▼ E - Describe malicious code and outline various types of malicious code

HSCJ 202

MISM 661

- ▼ E - Describe techniques for protection from malicious code to users, and provide examples (real and theoretical)

HSCJ 202

MISM 661

- ▼ *E - Define malicious code

HSCJ 202

MISM 661

▼ **(5) Access Controls**

- ▼ E - Define need-to-know

HSCJ 202

MISM 661

- ▼ E - Define risk management policy

HSCJ 202

MISM 661

- ▼ E - Explain user access policy

HSCJ 202

MISM 661

- ▼ E - Explain user access requirements

HSCJ 202

MISM 661

- ▼ *E - Define need to understand policy

HSCJ 202

MISM 661

▼ **D. CULTURE AND ETHICS**

▼ **(1) Policy**

- ▼ E - Define roles, responsibilities, and organization (e.g., separation of duties)

HSCJ 202

MISM 661

- ▼ E - Identify basic management issues and their impact on information systems security program

HSCJ 202

MISM 665

MISM 661

- ▼*E - Define culture and ethics policy

HSCJ 202

MISM 661

▼ **(2) Organization Culture**

- ▼*E - Describe organization culture

HSCJ 202

MISM 665

MISM 661

▼ **(3) Basic/Generic Management Issues**

- ▼*E - Describe basic/generic management issues

HSCJ 202

MISM 665

MISM 661

▼ **(4) Agency-Specific Security Policies & Procedures**

- ▼ E - Identify security policy-making bodies

HSCJ 202

MISM 661

- ▼*E - Describe how effective security policies and procedures can reduce threats to information systems

HSCJ 202

MISM 661

▼ **E. INCIDENT RESPONSE**

▼ **(1) Concept of Operations (CONOP)**

- ▼*E - Define Concept of Operations (CONOP)

HSCJ 202

MISM 661

▼ **(2) Criminal Activity Preparedness Planning**

- ▼*E - Explain criminal activity preparedness planning policy

HSCJ 202

HSCJ 210

MISM 661

▼ **(3) Organizational/Agency Systems Emergency/Incident Response Team**

- ▼ E - Identify organizational/agency systems emergency/incident response team

HSCJ 202

HSCJ 210

MISM 661

- ▼ E - Interact with organizational/agency systems emergency/incident response team to resolve incidents

HSCJ 202

HSCJ 210

MISM 661

- ▼*E - Define organizational/agency systems emergency/incident response team

HSCJ 202

HSCJ 210

MISM 661

▼ **(4) Malicious Code**

- ▼ E - Describe malicious code and outline various types of malicious code

HSCJ 202

MISM 661

- ▼ E - Describe techniques for protection from malicious code to users, and provide examples (real and theoretical)

HSCJ 202

MISM 661

- ▼ *E - Define malicious code

HSCJ 202

HSCJ 210

MISM 661

▼ **2. IMPLEMENT SITE SECURITY POLICY**

▼ **A. CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY (CIA)**

▼ **(2) Emergency Destruction Procedures (EDP)**

- ▼ *E - Discuss current emergency destruction plan (EDP) with necessary parties

HSCJ 202

MISM 661

▼ **(3) Continuity Plans**

- ▼ E - Describe accounting process for hardware, software, and information

HSCJ 202

MISM 661

- ▼ E - Outline accountability process/program

HSCJ 202

MISM 661

- ▼ *E - Address recovery procedures with SA/staff

HSCJ 202

MISM 661

- ▼ *E - Define who has responsibility for accountability

HSCJ 202

MISM 661

▼ **(4) Disposition of Classified Material**

- ▼ E - Explain the maintenance of audit records

HSCJ 202

MISM 661

- ▼ *E - Address disposition procedures with system administrator SA/staff

HSCJ 202

MISM 661

▼ **(5) Monitoring and Auditing**

- ▼ E - Address work force auditing and logging management procedures

HSCJ 202

MISM 661

- ▼ E - Discuss alarms, signals, and reports requirements

HSCJ 202

MISM 661

- ▼ E - Discuss auditing and logging management policies, laws, and penalties with personnel

HSCJ 202

MISM 661

- ▼ E - Discuss current auditing and logging management with necessary parties

HSCJ 202

MISM 661

- ▼*E - Address auditing and logging management with SA/staff

HSCJ 202

MISM 661

▼ **(7) Intrusion Detection**

- ▼ E - Address SA/staff about monitoring and auditing intrusion detection policies

HSCJ 202

MISM 661

- ▼ E - Address work force about intrusion detection management procedures

HSCJ 202

MISM 661

- ▼*E - Address intrusion detection management with SA/staff

HSCJ 202

MISM 661

▼ **(8) Investigation of Security Breaches**

- ▼*E - Define security breaches

HSCJ 202

MISM 661

▼ **(9) Monitoring**

- ▼ E - Address SA/staff about legal monitoring restrictions

HSCJ 202

MISM 661

- ▼ E - Address work force about monitoring management procedures

HSCJ 202

MISM 661

- ▼*E - Address monitoring management with SA/staff

HSCJ 202

MISM 661

▼ **(10) Configuration Management**

- ▼ E - Address SA/staff about legal configuration restrictions

HSCJ 202

MISM 661

- ▼ E - Address work force about configuration management procedures

HSCJ 202

MISM 661

- ▼*E - Address configuration management with SA/staff

HSCJ 202

MISM 661

▼ **(11) Countermeasures**

- ▼ E - Define cryptographic concepts

HSCJ 202

HSCJ 315

MISM 661

- ▼ E - Define digital signatures/non-repudiation
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ E - Define key management
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ E - Define message digests (e.g., MD5, SHA, HMAC)
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ E - Define methods of encryption
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ E - Identify protective technologies
 - HSCJ 202
 - MISM 661
- ▼ *E - Define cryptanalytic techniques
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ *E - Discuss intrusion detection problems
 - HSCJ 202
 - MISM 661

▼ **B. ENSURE FACILITY IS APPROVED**

▼ (Not Categorized)

- ▼ E - Define an approved service
 - HSCJ 202
 - MISM 661
- ▼ *E - Define an approved facility
 - HSCJ 202
 - MISM 661

▼ **C. OPERATIONS**

▼ (2) Agency/Vendor Cooperation/Coordination

- ▼ E - Explain agency policy for access by uncleared individuals and vendors to the SA and SSM viz., CIO, DAA, CTO, etc.
 - HSCJ 202
 - MISM 661
- ▼ E - Explain cooperation concerns to vendors
 - HSCJ 202
 - MISM 661
- ▼ E - Explain cooperation concerns with vendors to SSM, viz., CIO, DAA, CTO, etc.
 - HSCJ 202
 - MISM 661
- ▼ E - Facilitate agency control of access by uncleared individuals and vendors

HSCJ 202

MISM 661

- ▼ E - Facilitate correct agency redeployment of classified systems

HSCJ 202

MISM 661

- ▼ E - Facilitate vendor cooperation

HSCJ 202

MISM 661

- ▼ *E - Describe agency policy for redeploying classified systems to the SA and SSM viz., CIO, DAA, CTO, etc.

HSCJ 202

MISM 661

▼ **(3) Certification Advocacy**

- ▼ E - Explain advocacy role

HSCJ 202

MISM 661

- ▼ *E - Define advocacy

HSCJ 202

MISM 661

▼ **(4) Conduct Risk Assessment**

- ▼ E - Define risk assessment

HSCJ 202

MISM 661

- ▼ E - Describe risk assessment process

HSCJ 202

MISM 661

- ▼ E - Describe three states of information

HSCJ 202

MISM 661

- ▼ *E - Define information valuation

HSCJ 202

MISM 661

▼ **(5) Contracting for Security Services**

- ▼ E - Explain security services to contracting officers

HSCJ 202

MISM 661

- ▼ *E - Define an approved service

HSCJ 202

MISM 661

▼ **(7) Life Cycle System Security Planning**

- ▼ E - Describe agency policy for redeploying classified systems

HSCJ 202

MISM 661

- ▼ E - Explain life cycle security planning

HSCJ 202

MISM 661

- ▼ E - Explain life cycle system security planning

HSCJ 202

MISM 661

- ▼*E - Define life cycle security

HSCJ 202

MISM 661

▼ **(8) System Security Architecture Study**

- ▼E - Define system security architecture

HSCJ 202

MISM 661

- ▼E - Explain system security architecture study

HSCJ 202

MISM 661

- ▼*E - Address system security architecture study

HSCJ 202

MISM 661

▼ **D. GENERAL PRINCIPLES**

▼ **(1) Access Control Models**

- ▼*E - Discuss access control models

HSCJ 202

MISM 661

▼ **(2) Approval to Operate**

- ▼*E - Explain approval to operate

HSCJ 202

MISM 661

▼ **(3) Attack**

- ▼E - Explain attack root exploits

HSCJ 202

MISM 661

- ▼E - Explain backdoor routines

HSCJ 202

MISM 661

- ▼E - Explain denial-of-service (DOS) attacks

HSCJ 202

MISM 661

- ▼E - Explain remote explorer attack

HSCJ 202

MISM 661

- ▼E - Explain session hijacking tools

HSCJ 202

MISM 661

- ▼E - Explain war dialers

HSCJ 202

MISM 661

- ▼E - Explain war dialer/THC-scan attacks

HSCJ 202

MISM 661

- ▼*E - Explain attack

HSCJ 202

MISM 661

▼ **(4) Business Aspects of Information Security**

- ▼*E - Explain business aspects of information security

HSCJ 202

MISM 665

MISM 661

▼ **(6) Computer Network Attack**

- ▼*E - Explain computer network attack

HSCJ 202

MISM 661

▼ **(7) Criminal Prosecution**

- ▼*E - Explain criminal prosecution

HSCJ 202

MISM 661

▼ **(8) Defense in Depth**

- ▼*E - Give examples of defense in depth methods

HSCJ 202

MISM 661

▼ **(9) Due Care**

- ▼E - Monitor adherence to due care rules

HSCJ 202

MISM 661

- ▼E - Remind users of due care rules

HSCJ 202

MISM 661

- ▼*E - Address questions from users about due care

HSCJ 202

MISM 661

▼ **(10) Education, Training, & Awareness**

- ▼E - Recognize AT&E is a countermeasure

HSCJ 202

MISM 661

- ▼*E - List topics for inclusion into education, training and awareness plan

HSCJ 202

MISM 661

▼ **(11) Industrial Security**

- ▼*E - Explain industrial security

HSCJ 202

ISIN 330

MISM 661

▼ **(12) Information Warfare (INFOWAR) Concepts**

- ▼*E - Explain INFOWAR concepts

HSCJ 202

ISIN 330

MISM 661

▼ **(13) Intellectual Property Rights**

- ▼*E - Explain intellectual property rights
 - HSCJ 202
 - MISM 661
- ▼(14) Interim Approval to Operate (IATO)
 - ▼*E - Explain interim approval to operate
 - HSCJ 202
 - MISM 661
- ▼(15) Investigative Authorities
 - ▼*E - Explain investigative authorities
 - HSCJ 202
 - HSCJ 210
 - MISM 661
- ▼(16) Knowledge of Security Laws
 - ▼E - Discuss computer crime and the various methods
 - HSCJ 202
 - MISM 661
 - ▼E - Discuss Computer Fraud and Abuse Act
 - HSCJ 202
 - MISM 661
 - ▼E - Discuss Computer Security Act
 - HSCJ 202
 - MISM 661
 - ▼E - Discuss Copyright Law of the United States and related laws
 - HSCJ 202
 - MISM 661
 - ▼E - Discuss Copyright protection and licenses
 - HSCJ 202
 - MISM 661
 - ▼E - Discuss Electronic Freedom of Information Act
 - HSCJ 202
 - MISM 661
 - ▼E - Discuss Electronic Records Management and Federal Records Act
 - HSCJ 202
 - MISM 661
 - ▼E - Discuss Federal Information System Management Act
 - HSCJ 202
 - MISM 661
 - ▼E - Discuss Federal Managers Financial Integrity Act
 - HSCJ 202
 - HSCJ 317
 - MISM 661
 - ▼E - Discuss Federal Property and Administration Service Act
 - HSCJ 202
 - MISM 661
 - ▼E - Discuss Freedom of Information Act
 - HSCJ 202
 - MISM 661
 - ▼E - Discuss Government Information Security Reform Act

HSCJ 202

MISM 661

- ▼ E - Discuss Government Paperwork Elimination Act/Paperwork Reduction Act

HSCJ 202

MISM 661

- ▼ E - Discuss international legal issues which can affect Information Assurance

HSCJ 202

ISIN 330

MISM 661

- ▼ E - Discuss Millennium Copyright Act

HSCJ 202

MISM 661

- ▼ E - Discuss National Archives and Records Act

HSCJ 202

MISM 661

- ▼ E - Discuss Privacy Act/Privacy Act issues

HSCJ 202

MISM 661

- ▼ E - Discuss the legal responsibilities of the SSM, viz., CIO, DAA, CTO, etc.

HSCJ 202

MISM 661

- ▼ E - Discuss USA Patriot Act

HSCJ 202

ISIN 330

MISM 661

- ▼ *E - Discuss Clinger-Cohen Act

HSCJ 202

MISM 661

▼ **(17) Lattice Model**

- ▼ *E - Define lattice model

HSCJ 202

MISM 661

▼ **(18) Law Enforcement Interfaces**

- ▼ *E - Explain law enforcement interfaces

HSCJ 202

HSCJ 210

MISM 661

▼ **(20) Need for System Certification**

- ▼ *E - Explain need for system certification

HSCJ 202

MISM 661

▼ **(21) Operating Security Features**

- ▼ *E - Explain operating security features

HSCJ 202

MISM 661

▼ **(22) Risk Management**

- ▼ *E - Explain risk management

HSCJ 202

MISM 661

▼ **(23) Security Awareness as a countermeasure**

- ▼*E - Define security awareness for information system users

HSCJ 202

MISM 661

▼ **(24) Security Education as a countermeasure**

- ▼*E - Encourage employees to seek education in IA as a countermeasure

HSCJ 202

MISM 661

▼ **(25) Security Training as a countermeasure**

- ▼*E - Define security training for information system users

HSCJ 202

MISM 661

▼ **(26) Software Licensing**

- ▼*E - Explain software licensing

HSCJ 202

MISM 661

▼ **(27) Software Piracy**

- ▼*E - Explain software piracy

HSCJ 202

MISM 661

▼ **(28) Systems Security Authorization Agreement (SSAA)**

- ▼*E - Explain SSAA

HSCJ 202

MISM 661

▼ **(29) Systems Security Plan (SSP)**

- ▼*E - Explain Systems Security Plan (SSP)

HSCJ 202

MISM 661

▼ **(30) Standards of Conduct**

- ▼*E - Explain standards of conduct

HSCJ 202

MISM 661

▼ **(32) Waive Policy to Continue Operation**

- ▼*E - Explain Waive Policy to Continue Operation

HSCJ 202

MISM 661

▼ **E. SECURITY MANAGEMENT**

▼ **(1) Electronic Records Management**

- ▼ E - Define underlying rules for electronic records management program

HSCJ 202

MISM 661

- ▼ E - Describe the effect of electronic records management on the system

HSCJ 202

MISM 661

- ▼*E - Define electronic records management program and tools

HSCJ 202

MISM 661

▼ **(2) Records Retention**

- ▼ E - Define underlying rules for electronic records retention program

HSCJ 202

MISM 661

- ▼ E - Describe effect of records retention system

HSCJ 202

MISM 661

- ▼ E - List use of record retention

HSCJ 202

MISM 661

- ▼ *E - Discuss electronic records retention program

HSCJ 202

MISM 661

▼ **(3) E-Mail**

- ▼ E - Describe e-mail retention policies as they apply to system

HSCJ 202

MISM 661

- ▼ E - Describe e-mail system and its potential vulnerabilities

HSCJ 202

MISM 661

- ▼ E - Describe e-mail system/e-mail system security

HSCJ 202

MISM 661

- ▼ E - Discuss appropriate laws and policies for e-mail monitoring

HSCJ 202

MISM 661

- ▼ E - Explain e-mail monitoring management with SA/staff

HSCJ 202

MISM 661

- ▼ *E - Address SA/staff about legal e-mail monitoring restrictions

HSCJ 202

MISM 661

▼ **(4) Non-Repudiation**

- ▼ *E - Describe non-repudiation and its application to system

HSCJ 202

MISM 661

▼ **(5) Hardware Asset Management**

- ▼ E - Describe agency policy for redeploying classified systems

HSCJ 202

MISM 661

- ▼ E - Describe hardware asset management program

HSCJ 202

MISM 661

- ▼ E - Describe hardware asset management program and how it applies and is used on the system

HSCJ 202

MISM 661

- ▼*E - Describe agency policy for access by uncleared individuals and vendors

HSCJ 202

MISM 661

▼ **(6) Software Asset Management**

- ▼ E - Describe agency policy for redeploying classified systems

HSCJ 202

MISM 661

- ▼ E - Describe software asset management program

HSCJ 202

MISM 661

- ▼ E - Describe software asset management program and how it applies and is used on the system

HSCJ 202

MISM 661

- ▼ E - Describe software asset management program and how it applies/is used on system with emphasis on license and copyright issues, and cross reference to ethics

HSCJ 202

MISM 661

- ▼*E - Describe agency policy for access by uncleared individuals and vendors

HSCJ 202

MISM 661

▼ **F. ACCESS CONTROLS**

▼ **(1) Human Access**

- ▼ E - Address access management with SA/staff

HSCJ 202

MISM 661

- ▼ E - Address SA/staff about legal access restrictions

HSCJ 202

MISM 661

HSCJ 202

MISM 661

HSCJ 202

MISM 661

- ▼ E - Address work force about access control software management procedures

HSCJ 202

MISM 661

- ▼ E - Address work force about access management procedures

HSCJ 202

MISM 661

HSCJ 202

MISM 661

- ▼ E - Address work force about account management procedures

HSCJ 202

MISM 661

- ▼ E - Address work force about authentication procedures

- HSCJ 202
MISM 661

▼ E - Address work force authentication procedures
- HSCJ 202
MISM 661

▼ E - Describe agency policy for access by uncleared individuals and vendors
- HSCJ 202
MISM 661

▼ E - Discuss access control software management policies, laws and penalties with personnel
- HSCJ 202
MISM 661

▼ E - Discuss authentication policies, laws, and penalties with personnel
- HSCJ 202
MISM 661

▼ E - Discuss biometric access management policies, laws and penalties with personnel
- HSCJ 202
MISM 661

▼ E - Discuss current access control software management with necessary parties
- HSCJ 202
MISM 661

▼ E - Discuss current authentication with necessary parties
- HSCJ 202
MISM 661

▼ E - Discuss current biometric access management with necessary parties
- HSCJ 202
MISM 661

▼ E - Discuss current password management with necessary parties
- HSCJ 202
MISM 661

▼ E - Discuss password management policies, laws, and penalties with personnel
- HSCJ 202
MISM 661

▼ E - Discuss unauthorized access policies, laws, and penalties with personnel
- HSCJ 202
MISM 661

▼ *E - Address access control software management with SA/staff
- HSCJ 202
MISM 661

▼ *E - Address access management with SA/staff
- HSCJ 202
MISM 661

▼ *E - Address account management with SA/staff
- HSCJ 202
MISM 661

▼ *E - Address authentication with SA/staff

HSCJ 202

MISM 661

- ▼*E - Address biometric access management with SA/staff

HSCJ 202

MISM 661

- ▼*E - Address password management with SA/staff

HSCJ 202

MISM 661

- ▼*E - Address unauthorized access incident reporting with SA/staff

HSCJ 202

MISM 661

▼(2) Key Management

- ▼E - Demonstrate knowledge of how to operate a PKI system

HSCJ 202

HSCJ 315

MISM 661

- ▼E - Demonstrate knowledge of how to operate an EKMS system

HSCJ 202

HSCJ 315

MISM 661

- ▼E - Describe to users and managers what EKMS is, and how/why it is used

HSCJ 202

HSCJ 315

MISM 661

- ▼E - Describe to users and managers what key management is, and how/why EKMS is used

HSCJ 202

HSCJ 315

MISM 661

- ▼E - Describe to users and managers what key management is, and how/why PKI is used

HSCJ 202

HSCJ 315

MISM 661

- ▼E - Describe to users and managers what PKI is, and how/why it is used

HSCJ 202

HSCJ 315

MISM 661

- ▼E - Explain national key escrow policies and procedures

HSCJ 202

HSCJ 315

MISM 661

- ▼E - Identify components of EKMS as it applies to system

HSCJ 202

HSCJ 315

MISM 661

- ▼E - Identify components of PKI as it applies to system

- HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ E - Identify COMSEC
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ E - Identify EKMS requirements
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ E - Identify peer-to-peer requirements
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ E - Identify PKI requirements
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ E - Identify use for COMSEC material on system
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ E - Integrate services and advice of COMSEC Manager (Custodian) with operations
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ E - List national COMSEC policies
 - HSCJ 202
 - MISM 661
- ▼ E - List national COMSEC procedures
 - HSCJ 202
 - MISM 661
- ▼ E - Outline EKMS national policies and procedures and explain their relevance to users
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ E - Outline EKMS policies and procedures and explain their relevance to users
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ E - Outline national & agency EKMS management policies and procedures, and explain their relevance to users
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ E - Outline national & agency PKI management policies and procedures, and explain their relevance to users

- HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ E - Outline PKI national policies and procedures and explain their relevance to users
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ E - Outline PKI policies and procedures and explain their relevance to users
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ E - Submit EKMS requirements
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ E - Submit PKI requirements
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ E - Use EKMS management in a system
 - HSCJ 202
 - MISM 661
- ▼ E - Use key escrow management in a system
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ E - Use PKI management in a system
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ *E - Define EKMS
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ *E - Define KMI
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ *E - Define peer-to-peer
 - HSCJ 202
 - MISM 661
- ▼ *E - Define Public Key Infrastructure (PKI)
 - HSCJ 202
 - HSCJ 315
 - MISM 661
- ▼ *E - Describe to users and managers what key escrow is, and how/why it is used
 - HSCJ 202
 - HSCJ 315
 - MISM 661

- ▼*E - Explain to users and managers what COMSEC process is and how COMSEC process is relevant to them

HSCJ 202

HSCJ 315

MISM 661

▼ **G. INCIDENT RESPONSE**

▼ **Security Investigation Procedures**

- ▼ E - Describe process of investigating security incident

HSCJ 202

HSCJ 210

MISM 661

- ▼ E - Follow procedures

HSCJ 202

HSCJ 210

MISM 661

- ▼ E - Identify investigating authorities

HSCJ 202

HSCJ 210

MISM 661

- ▼*E - Assist in investigations as requested

HSCJ 202

HSCJ 210

MISM 661

▼ **3. ENFORCE AND VERIFY SYSTEM SECURITY POLICY**

▼ **A. CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY/ACCOUNTABILITY (CIA)**

▼ **(1) Planning**

- ▼*E - Discuss contingency plans

HSCJ 202

MISM 661

- ▼*E - Discuss continuity plans

HSCJ 202

MISM 661

- ▼*E - Discuss disposition of classified material & EDP

HSCJ 202

MISM 661

- ▼*E - Discuss reconstitution plans

HSCJ 202

MISM 661

▼ **(2) Monitoring and Auditing**

- ▼ E - Define security breach

HSCJ 202

MISM 661

- ▼ E - Ensure legal requirements for monitoring are enforced

HSCJ 202

MISM 661

- ▼ E - Explain consequences of unapproved monitoring

HSCJ 202

MISM 661

- ▼ E - Identify potential monitoring problems
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ *E - Define keystroke monitoring
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ *E - Discuss alarms, signals, and reports requirements
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ *E - Discuss intrusion detection problems
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ *E - Discuss network monitoring problems
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ *E - Discuss security breaches
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **(3) Environmental Controls**
 - ▼ *E - Discuss environmental control issues
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **(4) Filtered Power**
 - ▼ *E - Discuss filtered power issues
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **(5) Fire Prevention**
 - ▼ *E - Discuss fire prevention issues
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **(6) Grounding**
 - ▼ *E - Discuss grounding issues
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **(7) Safety**
 - ▼ *E - Discuss safety issues
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **C. ACCESS CONTROLS**
 - ▼ **(1) Human Access**
 - ▼ E - Describe agency policy for access by uncleared individuals and vendors
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼ *E - Discuss unauthorized access attempts
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼ *E - Verify requested access

HSCJ 202

MISM 661

- ▼*E - #Require users and system support personnel to have required security clearances, authorizations and need-to-know, and are indoctrinated before granting access

HSCJ 202

MISM 661

▼ **(2) Key Management**

- ▼ E - List national COMSEC procedures

HSCJ 202

HSCJ 315

MISM 661

- ▼*E - Explain national key escrow policies and procedures

HSCJ 202

MISM 661

- ▼*E - List national COMSEC policies

HSCJ 202

HSCJ 315

MISM 661

▼ **(3) Configuration Management**

- ▼*E - Identify configuration management requirements

HSCJ 202

MISM 661

▼ **(4) Protective Technology**

- ▼*E - Identify protective technology requirements

HSCJ 202

MISM 661

▼ **D. AUTOMATED SECURITY TOOLS**

▼ **(1) Automated Security Tools**

- ▼*E - Use expert system tools (i.e., audit reduction and intrusion detection) available

HSCJ 202

MISM 661

▼ **E. HANDLING MEDIA**

▼ **(6) Remanence**

- ▼*E - Execute non-automated data remanence tools

HSCJ 202

MISM 661

▼ **(8) Disposition of Classified Material**

- ▼ E - Define disposition reports

HSCJ 202

MISM 661

- ▼*E - Explain disposition of classified media policies and procedures

HSCJ 202

MISM 661

▼ **F. INCIDENT RESPONSE**

▼ **(1) Criminal Prosecution**

- ▼*E - Discuss criminal prosecution requirements

HSCJ 202

MISM 661

▼ **(4) Legal and Liability Issues**

- ▼ E - Identify legal liability issues

HSCJ 202

MISM 661

- ▼ *E - Discuss legal liability issues

HSCJ 202

MISM 661

▼ **4. REPORT ON SITE SECURITY STATUS**

▼ **A. SECURITY CONTINUITY REPORTING**

▼ **(1) Contingency Plans**

- ▼ *E - Define contingency plan reporting

HSCJ 202

MISM 661

▼ **(2) Continuity Plans**

- ▼ E - Define backup reports

HSCJ 202

MISM 661

- ▼ E - Define reconstitution reporting

HSCJ 202

MISM 661

- ▼ *E - Define continuity plan reporting

HSCJ 202

MISM 661

- ▼ *E - Define restoration reports

HSCJ 202

MISM 661

▼ **(3) Disposition of Classified Material & Emergency Destruction Procedures (EDP)**

- ▼ E - Define EDP reports

HSCJ 202

MISM 661

- ▼ *E - Define disposition reports

HSCJ 202

MISM 661

▼ **(4) Monitoring and Auditing**

- ▼ *E - Explain how to report audit assessments

HSCJ 202

MISM 661

- ▼ *E - Explain reporting audit alarms and signals

HSCJ 202

MISM 661

▼ **(5) Identification & Authentication**

- ▼ *E - Describe process to report insufficient passwords

HSCJ 202

MISM 661

- ▼*E - Describe process to report unauthorized accounts

HSCJ 202

MISM 661

- ▼ **(6) Configuration Management**

- ▼*E - Describe configuration management reporting requirements

HSCJ 202

MISM 661

- ▼ **(7) Testing**

- ▼*E - Describe how various types of testing are reported

HSCJ 202

MISM 661

- ▼ **B. REPORT SECURITY INCIDENTS**

- ▼ **(1) Computer Organizational/Agency Systems Emergency/Incident Response Team**

- ▼E - Distribute organizational/agency systems emergency/incident response team reports and advisories

HSCJ 202

HSCJ 210

MISM 661

- ▼*E - Identify organizational/agency systems emergency/incident response team

HSCJ 202

HSCJ 210

MISM 661

- ▼ **(3) Security Violations Reporting Process (incident response)**

- ▼*E - Comply with agency specific/local directives when reporting to SSM, viz., CIO, DAA, CTO, etc.

HSCJ 202

HSCJ 210

MISM 661

- ▼ **C. LAW**

- ▼ **(1) Investigative Authorities**

- ▼*E - Identify agencies and offices responsible for investigating security incidents

HSCJ 202

MISM 661

- ▼ **(2) Law Enforcement Interfaces (LEI)**

- ▼E - Describe how to contact law enforcement interfaces (LEI)

HSCJ 202

MISM 661

- ▼*E - Describe how ISSO interfaces with law enforcement agencies

HSCJ 202

HSCJ 210

MISM 661

- ▼ **(3) Witness Interviewing/Interrogation**

- ▼E - Describe proper procedures to follow when conducting a witness interview

HSCJ 202

HSCJ 210

MISM 661

- ▼E - Identify who can conduct interrogations (investigative agencies only)

HSCJ 202

HSCJ 210

MISM 661

- ▼ *E - Assist appropriate authority in witness interviewing/interrogation

HSCJ 202

HSCJ 210

MISM 661

▼ **(5) Disgruntled Employees**

- ▼ *E - Identify notification requirements for handling disgruntled employees

HSCJ 202

MISM 661

▼ **D. REPORT SECURITY STATUS OF INFORMATION SYSTEM AS REQUIRED BY SSM, VIZ., CIO, DAA, CTO, ETC.**

▼ **(1) Administrative Security Policies and Procedures**

- ▼ *E - Explain necessity of reporting on administrative security policies and practices

HSCJ 202

MISM 661

▼ **(2) Agency Specific Security Policies**

- ▼ *E - Describe how agency specific policies enhance overall security posture of information systems by defining operational environment

HSCJ 202

MISM 661

▼ **(3) Organizational/Agency Systems Emergency/Incident Response Team**

- ▼ *E - Explain how other sources of information can assist ISSO in providing additional information for reporting security status of information systems

HSCJ 202

MISM 661

▼ **(4) Automated Systems Security Incident Support Team (ASSIST)**

- ▼ *E - Explain how other sources of information can assist ISSO in providing additional information for reporting security status of information systems

HSCJ 202

MISM 661

▼ **(5) Trade Journals, Bulletin Board System (BBS) Notices**

- ▼ *E - Explain how other sources of information can assist ISSO in providing additional information for reporting security status of information systems

HSCJ 202

MISM 661

▼ **E. REPORT TO IG**

▼ **Inspector General (IG) (External) Audit & Assessments**

- ▼ E - Identify appropriate reporting channels for IG

HSCJ 202

MISM 661

- ▼ *E - Describe areas encompassed by report

HSCJ 202

MISM 661

▼ **5. SUPPORT CERTIFICATION AND ACCREDITATION**

▼ **A. CERTIFICATION FUNCTION**

- ▼ **(1) Assessments (e.g., surveys, inspections)**

- ▼*E - Prepare assessments for use during certification of information systems

HSCJ 202

MISM 661

▼ **B. ACCREDITATION FUNCTION**

▼ **(1) ISSO**

- ▼ E - Initiate accreditation process

HSCJ 202

MISM 661

- ▼*E - Monitor system status post accreditation

HSCJ 202

MISM 661

▼ **(3) System Administrator (SA)**

- ▼*E - Explain contents of Systems Security Plan (SSP)

HSCJ 202

MISM 661

▼ **C. RESPOND TO SSM, VIZ., CIO, DAA, CTO, ETC. REQUESTS**

▼ **(1) Approval to Operate**

- ▼*E - Explain purpose and contents of Approval to Operate (ATO) to users

HSCJ 202

MISM 661

▼ **(2) Assessment Methodology**

- ▼*E - Explain C&A process for information system

HSCJ 202

MISM 661

▼ **(3) Certification Statement**

- ▼*E - Explain purpose and contents of Certification Statement to users

HSCJ 202

MISM 661

▼ **(4) Certification Tools**

- ▼ E - Discuss ST&E plan and procedures

HSCJ 202

MISM 661

- ▼ E - Recommend revisions to ST&E plan and procedures

HSCJ 202

MISM 661

- ▼ E - Recommend use of specific certification tools

HSCJ 202

MISM 661

- ▼*E - Discuss certification tools

HSCJ 202

MISM 661

▼ **(5) Identify Security Changes to SSM, viz., CIO, DAA, CTO, etc.**

- ▼ E - Explain security-relevant changes to be made to information system

HSCJ 202

MISM 661

- ▼*E - Differentiate security-related changes from non-security-related changes

HSCJ 202

MISM 661

▼ **(6) Interim Approval to Operate (IATO)**

- ▼ *E - Explain purpose and contents of Interim Approval to Operate (IATO) to users

HSCJ 202

MISM 661

▼ **(7) Re-Certification**

- ▼ E - Identify information system that needs re-certification

HSCJ 202

MISM 661

- ▼ *E - Explain purpose and process of re-certification

HSCJ 202

MISM 661

▼ **(8) Security Test & Evaluation (ST&E)**

- ▼ *E - Discuss ST&E

HSCJ 202

MISM 661

▼ **(9) SSAA**

- ▼ *E - Explain contents of SSAA

HSCJ 202

MISM 661

▼ **(10) Type Accreditation**

- ▼ *E - Explain purpose and contents of type accreditation to users

HSCJ 202

MISM 661

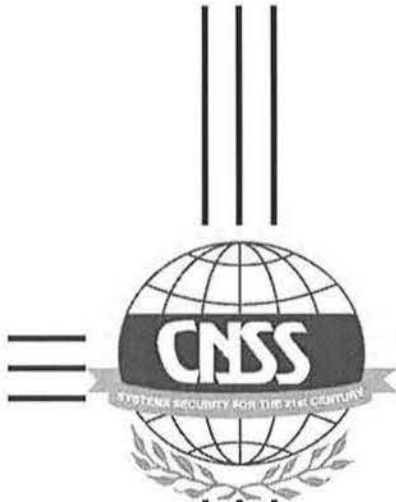
▼ **(11) Waive Policy to Continue Operation**

- ▼ *E - Explain justification for waiver

HSCJ 202

MISM 661

b. Standard Specifications



**NATIONAL INFORMATION
ASSURANCE TRAINING STANDARD
FOR
INFORMATION SYSTEMS SECURITY
OFFICERS**

Awareness, Training, and Education (AT&E) are cost-effective methods of improving organizational Information Assurance (IA). In times of ever-contracting budgets, it is difficult to persuade management to spend money on security and training activities that have no direct impact on the organizational bottom line. This paper describes the process used to aid in the systematic development of training to serve as the first line of defense in Information Assurance (IA). In addition, it describes how these materials are applicable to your organizational long-range plans.

This document provides minimum standards for Information Systems Security Officers responsible for national security systems. It also may offer guidelines for Systems Security Officers responsible for unclassified systems. Your department or agency may require a more stringent implementation.



COMMITTEE ON NATIONAL SECURITY SYSTEMS
NATIONAL MANAGER

FOREWORD

1. Since the September 11th Terrorist Attacks against the sovereignty of the United States and its people, both the President and the Congress have redoubled their efforts to underpin the nation's security. The following guidance, reflecting their support, is intended to assist all federal agencies and the private sector concerned with protecting their information systems. Only through diligence and a well-trained workforce will we be able to adequately defend the nation's vital information resources.

2. CNSSI No. 4014 is effective upon receipt. It replaces the National Training Standard for Information Systems Security Officers (ISSO), dated August 1997, which should be destroyed.

3. This instruction establishes the minimum course content or standard for the development and implementation of Information Assurance (IA) training for Information Systems Security Officers (ISSOs). Please check with your agency for applicable implementing documents.

4. Representatives of the Committee on National Security Systems (CNSS) may obtain additional copies of this instruction from:

NATIONAL SECURITY AGENCY
CNSS SECRETARIAT
ATTN: I01C STE 6716
FORT GEORGE G. MEADE, MD 20755-6716

/s/

MICHAEL V. HAYDEN
Lieutenant General, USAF

**NATIONAL TRAINING STANDARD
FOR
INFORMATION SYSTEMS SECURITY OFFICER (ISSO)**

	<u>SECTION</u>
PURPOSE	I
APPLICABILITY	II
RESPONSIBILITIES	III

SECTION I – PURPOSE

- 1) This instruction establishes the minimum training standard for the development and implementation of training for an Information Systems Security Officer (ISSO) in Information Assurance (IA).

SECTION II – APPLICABILITY

- 2) The National Security Telecommunications and Information Systems Security Directive (NSTISSD) No. 501 establishes the requirement for federal departments and agencies to implement training programs for IA professionals. As defined in NSTISSD 501, an IA professional is an individual responsible for the security oversight or management of national security systems during phases of the life cycle of a given information system. That directive is being implemented in a synergistic environment among departments and agencies that are committed to satisfying these IA education and training requirements in the most effective and efficient manner possible. This instruction is the continuation of a series of minimum training and education standards being developed to assist departments and agencies in meeting their responsibilities in these areas (NSTISSI Nos. 4011, 4012, 4013, and 4015). The definitions for words used in this instruction are derived from the National Information Assurance (IA) Glossary, NSTISSI No. 4009. The references pertinent to this instruction are listed in ANNEX B.
- 3) The body of knowledge listed in this instruction was obtained from a variety of sources; i.e., industry, government, and academia. ANNEX A lists the minimal IA performance standard for an ISSO.
- 4) This instruction is applicable to all departments and agencies of the U.S. Government and their contractors responsible for the development and implementation of training for ISSOs in the IA discipline.

SECTION III – RESPONSIBILITIES

- 5) Heads of U.S. Government departments and agencies shall ensure that ISSOs are made aware of the body of knowledge outlined in this instruction, and that such training is provided to those requiring it at the earliest practicable date.
- 6) The National Manager shall:
 - maintain and provide an IA training standard for ISSOs to U.S. Government departments and agencies;
 - ensure that appropriate IA training courses for ISSOs are developed; and
 - assist other U.S. Government departments and agencies in developing and/or conducting IA training activities for ISSOs as requested.

Enclosures:

Annex A

Annex B

ANNEX A

**INFORMATION ASSURANCE (IA) PERFORMANCE STANDARD FOR THE ISSO
(ENTRY, INTERMEDIATE, & ADVANCED LEVELS)**

Job functions using competencies identified in:

DoDD 8500.2, Information Assurance Implementation

Common Criteria for Information Technology Security Evaluation

DCID 6/3, Protecting Sensitive Compartmented Information Within Information Systems

The IA functions of an ISSO are:

- 1) maintaining a plan for site security improvements and progress towards meeting accreditation;
- 2) ensuring the information system (IS) is operated, used, maintained, and disposed of in accordance with security policies and practices;
- 3) ensuring the IS is certified and accredited;
- 4) ensuring users and system support personnel have required security clearances, authorization and need-to-know, are indoctrinated, and are familiar with internal security practices before access to the IS is granted;
- 5) enforcing security policies and safeguards on personnel having access to an IS for which the ISSO is responsible;
- 6) ensuring audit trails are reviewed periodically (e.g., weekly, daily), and audit records are archived for future reference, if required;
- 7) initiating protective or corrective measures;
- 8) reporting security incidents in accordance with agency-specific policy, such as DoDD 8500.2, to the Senior System Manager (SSM), viz., Chief Information Officer (CIO), Designated Approving Authority (DAA), Chief Technology Officer (CTO), etc., when the IS is compromised;
- 9) reporting security status of the IS, as required by the DAA; and
- 10) evaluating known vulnerabilities to ascertain if additional safeguards are needed.

Terminal Objective:

- **ENTRY LEVEL:** Given a series of system security breaches, the ISSO will identify system vulnerabilities and recommend security solutions required to return systems to an operational level of assurance.
- **INTERMEDIATE LEVEL:** Given a proposed new system architecture requirement, the ISSO will investigate and document system security technology, policy, and training requirements to assure system operation at a specified level of assurance.
- **ADVANCED LEVEL:** Given a proposed IS accreditation action, the ISSO will analyze and evaluate system security technology, policy, and training requirements in support of the Senior System Manager (SSM), viz., Chief Information Officer (CIO), Designated Approving Authority (DAA), Chief Technology Officer (CTO), etc., approval to operate the system at a specified level of assurance. This analysis will include a description of the management/technology team required to successfully complete the accreditation process.

List of performance items under job functions

E = entry level
I = intermediate level
A = advanced level

In each of the competency areas listed below by job function, the ISSO shall perform the following functions at the levels indicated:

I. DEVELOP CERTIFICATION AND ACCREDITATION POSTURE

A. PLANNING FOR CERTIFICATION AND ACCREDITATION

(1) Planning

- E – Define certification and accreditation
- E – Explain Common Criteria (CC)
- E – Discuss National Information Assurance Program (NIAP) Validated Products List
- E – Explain Information Technology Security Evaluation Criteria (ITSEC)
- E – Explain International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17799
- E – Explain the Model for Information Assurance: An Integrated Approach (2nd Annual IEEE Systems, Man and Cybernetics Information Assurance Workshop, June 2002)
- E – Discuss goals, mission, and objectives of the organization(s)
- E – Discuss Information Technology Security Evaluation Criteria (ITSEC)
- E – Discuss the concepts of availability, integrity, confidentiality, authentication, and non-repudiation
- E – Discuss the theoretical concepts of security models – confidentiality models (e.g., Bell & LaPadula)
- E – Discuss the theoretical concepts of security models – commercial systems models
- E – Discuss the theoretical concepts of security models – integrity models (e.g., Biba, Clark and Wilson)
- E – Discuss the theoretical concepts of security models – information flow models
- E – Discuss the components of information systems evaluation models
- I – Analyze the constituent components of the certification and accreditation process
- E – Discuss the constituent components of the certification and accreditation process
- I – Develop policy for completing and maintaining certification and accreditation
- I – Explain certification and accreditation policy planning
- A – Develop site security policy
- A – Summarize planning for certification and accreditation posture
- A – Write plan for certification and accreditation policy

(2) Defense in Depth

- E – Give examples of defense in depth methods
- I – Discuss defense in depth
- I – Explain defense in depth
- I – Explain the Model for Information Assurance: An Integrated Approach (2nd Annual IEEE Systems, Man and Cybernetics Information Assurance Workshop, June 2002)
- I – Summarize defense in depth

A – Verify implementation of defense in depth

(3) Assets

- E – Define assets
- E – Define contracts, agreements, and other obligation policy
- E – Define policy for user roles
- E – Define system owner
- E – Define data owner
- E – Discuss user roles
- E – Identify assets
- E – Identify contracts, agreements, and other obligations
- E – Identify database structure
- E – Identify system owner
- E – Identify data owner
- E – Identify systems interconnection
- I – Explain asset inventory
- I – Explain contracts, agreements, and other obligation policy
- I – Explain database security feature use policy
- I – Explain systems interconnection policy
- I – Explain user roles
- I – Monitor systems interconnection
- I – Summarize asset inventory
- I – Summarize database security feature use policy
- I – Summarize systems interconnection policy
- A – Integrate database security feature use policy
- A – Verify asset inventory process
- A – Write asset inventory policy
- A – Write contracts, agreements, and other obligation policy
- A – Write database security feature use policy
- A – Write systems interconnection policy
- A – Interpret asset inventory report

(4) Threats

- E – Define adversarial threat
- E – Define aggregation
- E – Define technological threats
- E – Define threats from careless/disgruntled employees
- E – Define social engineering threats
- E – Describe how espionage (industrial/international) can impact security of information systems
- E – Describe adversarial threat
- E – Describe how people can threaten system’s security, i.e., intentional and unintentional
- E – Describe how security reviews can be used to identify threats to information systems
- E – Describe threat from electronic emanations
- E – Describe threat from natural sources (fire, flood, earthquake, etc)

- E – Describe types of environmental control (air conditioning, filtered power, etc.) threats
- E – Describe types of intentional human threats to system
- E – Describe types of unintentional human threats to system
- E – Discuss aggregation
- E – Discuss boundary
- E – Discuss application and system vulnerabilities and threats - web-based (e.g., XML, SAML)
- E – Discuss security implications posed by portable devices and components
- E – Discuss application and system vulnerabilities and threats - client-based (e.g., applets, Active-X)
- E – Discuss natural disaster impacts on system
- E – Discuss application and system vulnerabilities and threats - server-based
- E – Discuss application and system vulnerabilities and threats - mainframe
- E – Discuss application and system vulnerabilities and threats - malicious code (e.g., Trojan Horses, trap doors, viruses, worms)
- E – Discuss data mining
- E – Discuss databases and data warehousing vulnerabilities, threats and protections
- E – Discuss inference
- E – Discuss object reuse
- E – Discuss polyinstantiation
- E – Discuss perimeter and building grounds protection issues/systems
- E – Discuss access control attacks (brute force, dictionary, spoofing, denial of service, etc.)
- E – Discuss how the security architecture is affected by assurance and confidence
- E – Discuss how the security architecture is affected by covert channels
- E – Discuss how the security architecture is affected by countermeasures
- E – Discuss how the security architecture is affected by emanations
- E – Discuss how the security architecture is affected by maintenance hooks and privileged programs
- E – Discuss how the security architecture is affected by resource misuse prevention
- E – Discuss how the security architecture is affected by states attacks (e.g., time of check/time of use)
- E – Discuss how the security architecture is affected by timing attacks
- E – Identify access control attacks (brute force, dictionary, spoofing, denial of service, etc.)
- E – Identify appropriate EMSEC/TEMPEST authorities
- E – Identify process for evaluating threat
- E – Identify related disciplines that should contribute to risk analysis
- I – Discuss computer network attack threat
- I – Discuss data aggregation policy
- I – Explain careless employee policy
- I – Explain disgruntled employee policy
- I – Explain security review policy
- I – Explain social engineering policy
- I – Explain EMSEC/TEMPEST policy

- I – Identify computer network attack threats
- I – Identify sources of technological threats: hardware, software (operating systems, applications, malicious code), firmware, networks (local area networks, wide area networks, metropolitan area networks, and direct connect)
- I – Identify threat from aggregation
- I – Identify threats from related disciplines
- I – Present computer network attack policy
- I – Present computer network attack threat policy
- I – Present data aggregation policy
- I – Present facility management policy
- I – Present human threat policy
- I – Present security review policy
- I – Present social engineering policy
- I – Present EMSEC/TEMPEST policy
- I – Present threat assessment policy
- I – Summarize computer network attack policy
- I – Summarize computer network attack threat policy
- I – Summarize data aggregation policy
- I – Summarize facility management policy
- I – Summarize human threat policy
- I – Summarize security review policy
- I – Summarize social engineering policy
- I – Summarize EMSEC/TEMPEST policy
- I – Summarize threat assessment policy
- I – Use knowledge of threats from related disciplines
- A – Analyze threats
- A – Evaluate computer network attack threats
- A – Evaluate data aggregation policy
- A – Evaluate threat assessment
- A – Evaluate threat from aggregation
- A – Integrate data in to threat assessment
- A – Interpret security review
- A – Write careless/disgruntled employee monitoring policy
- A – Write computer network attack policy
- A – Write data aggregation policy
- A – Write disgruntled employee monitoring policy
- A – Write facility management policy
- A – Write human threat policy
- A – Write security review policy
- A – Write social engineering monitoring policy
- A – Write EMSEC/TEMPEST policy
- A – Write threat assessment plan
- A – Write threat assessment policy

(5) Vulnerabilities

- E – Assist in performance of vulnerability analysis
- E – Define National Information Assurance Program (NIAP) Validated Products List

- E – Define Protection Profiles
- E – Define vulnerabilities
- E – Describe agency/vendor cooperation/coordination
- E – Describe agency policy for access by uncleared individuals and vendors
- E – Describe agency policy for redeploying classified systems
- E – Describe technical surveillance vulnerabilities
- E – Describe vulnerability analysis
- E – Identify technical surveillance vulnerabilities
- I – Demonstrate how to use NIAP Validated Products
- I – Conduct/perform vulnerability analysis
- I – Discuss technical surveillance vulnerabilities
- I – Discuss technical surveillance vulnerabilities policy
- I – Evaluate vulnerability
- I – Explain agency/vendor cooperation/coordination policy
- I – Explain agency policy for access by uncleared individuals and vendors
- I – Explain agency policy for redeploying classified systems
- I – Explain Validated Products policy
- I – Explain Validated Products
- I – Explain Protection Profile policy
- I – Identify vulnerabilities with acquisitions
- I – Present security requirements
- I – Select vulnerabilities identified by agencies/vendors with existing cooperation/coordination
- I – Select vulnerabilities in agency policy for access by uncleared individuals and vendors
- I – Select vulnerabilities in agency policy for redeploying classified systems
- I – Summarize technical surveillance vulnerabilities policy
- I – Use Protection Profiles for input into vulnerability analysis
- A – Analyze results of vulnerability analysis
- A – Analyze vulnerabilities
- A – Compile recommended fixes for deficiencies identified by vulnerability analysis
- A – Recommend Evaluated Products for use in a system
- A – Write agency/vendor cooperation/coordination policy
- A – Write agency policy for access by uncleared individuals and vendors
- A – Write agency policy for redeploying classified systems
- A – Write Validated Product policy
- A – Write Protection Profile policy
- A – Write technical surveillance vulnerabilities policy
- A – Write vulnerability analysis policy

(6) Criticality

- E – Define asset criticality
- E – Define attack analysis
- E – Define criticality
- I – Develop asset criticality measures
- I – Identify asset criticality
- A – Assess criticality

- A – Write attack analysis plan
- A – Write attack analysis policy
- A – Write attack analysis report

(7) Risk

- E – Define risk (threat and vulnerability pairs together with significance)
- E – Discuss risk management concepts
- I – Develop risk policy
- I – Present risk policy
- A – Write risk policy

(8) Conduct Risk Assessment

- E – Define information valuation
- E – Define risk assessment
- E – Describe risk assessment process
- E – Describe three states of information
- I – Coordinate risk assessment process
- I – Develop policy and procedures for conducting a risk assessment
- I – Summarize risk profile
- I – Write risk assessment reports
- A – Coordinate resources to perform a risk assessment
- A – Interpret results of a risk assessment
- A – Interpret risk assessment report
- A – Perform security assessment
- A – Write risk assessment plan
- A – Write risk assessment policy

(9) Countermeasures

- E – Define countermeasures
- E – Describe how countermeasures can mitigate risk
- E – Discuss application environment and security controls
- E – Discuss audit trails/access logs & intrusion detection applications
- E – Discuss firewalls
- E – Discuss badging, and smart/dumb cards
- E – Discuss biometric access controls to facility
- E – Discuss CCTV requirements/capabilities
- E – Define National Information Assurance Program (NIAP) Validated Products List
- E – Discuss escort requirements/visitor control issues
- E – Discuss fire detection and suppression issues/systems
- E – Discuss intrusion detection system (e.g., firewalls, motion detectors, sensors, alarms) requirements/capabilities
- E – Discuss keys and locks requirements/capabilities
- E – Discuss power and HVAC considerations
- E – Discuss restricted areas/work areas security requirements
- E – Discuss risk management concepts
- E – Discuss security guard requirements
- E – Discuss site selection and facility design configuration considerations
- E – Discuss turnstiles and mantraps requirements

- E – Discuss water, leakage, flooding impact to system
- E – Identify countermeasures to deter/mitigate attack threats (e.g.; malicious code, flooding, spamming)
- I – Develop security plan
- I – Develop a security policy
- I – Explain ITSEC/Common Criteria
- I – Summarize countermeasure
- I – Summarize ITSEC/Common Criteria policy
- A – Ensure training for SA/staff with specific IT security roles is provided
- A – Evaluate information system security strategies
- A – Recommend accreditation of a system to the SSM, viz., CIO, DAA, CTO, etc. based on risk assessment
- A – Recommend actions to management based on risk acceptance
- A – Recommend ITSEC/Common Criteria policy

(10) Organizational/Agency Systems Emergency/Incident Response Team

- E – Define organizational/agency systems emergency/incident response team
- E – Identify organizational/agency systems emergency/incident response team

(11) Education, Training, & Awareness (ETA)

- E – List topics for inclusion into education, training, and awareness (ETA) policy
- E – Discuss ETA as a countermeasure
- I – Develop ETA policy
- I – Recommend input to organizational ETA activities

(12) Residual Risk

- E – Define residual risk
- I – Explain residual risk
- I – Summarize residual risk
- A – Write residual risk standard and policy

(13) Cost/Benefit Analysis

- E – Define cost/benefit analysis
- E – Define risk acceptance
- I – Conduct business impact analysis
- I – Conduct cost/benefit analysis procedures
- I – Describe cost of the system life cycle and security
- I – Describe risk acceptance process
- I – Summarize cost/benefit analysis
- A – Interpret cost/benefit analysis results to formulate recommend changes
- A – Recommend cost/benefit analysis
- A – Write cost/benefit analysis

B. CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY (CIA) POLICY

(1) Contingency Plans

- E – Define contingency plans
- E – Identify items for which plans must be developed
- E – Prepare input to contingency plan

- E – Write contingency plan
- I – Present contingency plan
- I – Specify method to exercise contingency plan
- I – Specify method to test contingency plan
- I – Exercise contingency plan
- I – Assess effectiveness of contingency plan

(2) Concept of Operations (CONOP)

- E – Define Concept Of Operations (CONOP)
- I – Develop CONOP policy
- I – Discuss information covered by CONOP
- I – Present CONOP plan
- I – Propose methods and policies to include in CONOP
- A – Integrate standard operating procedures into CONOP
- A – Write CONOP policy
- A – Write CONOP plan
- A – Develop/write roles and responsibilities for continuity participants

(3) Continuity Plans

- E – Define continuity plan
- E – Discuss business continuity planning (BCP)
- E – Discuss business organization analysis
- E – Discuss disaster recovery planning (DRP) (recovery planning and strategy)
- E – Discuss project scope development and planning
- E – Discuss resource requirements
- E – Identify items for which plans must be developed
- E – Outline security policy for backup procedures
- E – Prepare input to continuity plan
- E – Write continuity plan
- I – Develop alternatives - cold, warm, hot and mobile sites, electronic vaulting, etc
- I – Develop backups and off-site storage plan
- I – Develop business resumption plan
- I – Develop communications plan
- I – Develop documentation plan
- I – Develop emergency response plan
- I – Develop fire and water protection plan
- I – Develop logistics and supplies plan
- I – Develop personnel notification plan
- I – Develop processing agreements - reciprocal, mutual, etc
- I – Develop recovery strategy
- I – Develop unit priorities
- I – Develop utilities plan
- I – Explain business organization analysis
- I – Explain project scope development and planning
- I – Explain resource requirements
- I – Modify contingency plan reflecting changes
- I – Plan backups and off-site storage

- I – Plan business resumption
- I – Plan communications
- I – Plan documentation
- I – Plan emergency response
- I – Plan fire and water protection
- I – Plan logistics and supplies
- I – Plan personnel notification
- I – Plan primary/backup/reconstitution utilities
- I – Present continuity plan
- I – Review backup policy
- I – Specify method to exercise backup plan
- I – Specify method to exercise continuity plan
- I – Specify method to exercise reconstitution plan
- I – Specify method to test continuity plan
- I – Specify method to test reconstitution plan
- I – Test/exercise continuity plans
- I – Test/exercise reconstitution plans
- A – Develop/write backups and off-site storage plan
- A – Develop/write business resumption plan
- A – Develop/write communications plan
- A – Develop/write documentation plan
- A – Develop/write emergency response plan
- A – Develop/write fire and water protection plan
- A – Develop/write logistics and supplies plan
- A – Develop/write personnel notification plan
- A – Develop/write utilities plan
- A – Evaluate backup policy
- A – Integrate reconstitution plans into local policy

(4) Legal Plan

(a) Criminal Activity Preparedness Planning

- E – Discuss evidence collection and handling
- E – Discuss incident handling and response
- E – Discuss the parameters of investigations
- I – Explain NSTISSP 11
- I – Develop/write policy for criminal activity
- I – Explain criminal activity preparedness planning policy
- I – Explain evidence collection and handling
- I – Explain incident handling and response
- I – Explain the parameters of investigations
- I – Explain containment/management of evidence
- A – Evaluate criminal activity preparedness plan
- A – Integrate criminal activity preparedness into local policy
- A – Summarizes criminal activity preparedness plan
- A – Write policy for criminal activity

(b) Laws*

- E – Discuss Clinger-Cohen Act

- E – Discuss Computer Fraud and Abuse Act
- E – Discuss Copyright Act of 1976
- E – Discuss Copyright Protection and License
- E – Discuss Electronic Freedom of Information Act
- E – Discuss Electronic Records Management and Federal Records Act
- E – Discuss Federal Information System Management Act
- E – Discuss Federal Managers Financial Integrity Act
- E – Discuss Federal Property and Administration Service Act
- E – Discuss Freedom of Information Act
- E – Discuss Government Paperwork Elimination Act
- E – Discuss Government Information Security Reform Act
- E – Discuss Millennium Copyright Act
- E – Discuss National Archives and Records Act
- E – Discuss Privacy Act issues
- E – Discuss USA Patriot Act
- E – Discuss computer crime and various methods used to commit computer crime
- E – Discuss computer crime laws
- E – Discuss implications of the Privacy Act
- E – Discuss import/export laws
- E – Discuss information systems security laws
- E – Discuss intellectual properties laws
- E – Discuss international legal issues which can affect information assurance
- E – Discuss liability laws
- E – Discuss licensing laws
- E – Discuss legal responsibilities of the SSM, viz., CIO, DAA, CTO, etc.
- E – Discuss requirements of Computer Security Act
- E – Discuss trans-border data flow laws
- A – Verify applicable laws and directives

* As amended

(5) Disposition of Classified Material & Emergency Destruction Policy (EDP)

- E – Define disposition of classified material
- E – Explain emergency destruction policy (EDP) to those who execute plans
- I – Explain disposition policy
- I – Present disposition plan
- I – Specify method to exercise disposition plan
- I – Specify method to test disposition plan
- I – Summarize disposition policy
- A – Integrate EDP into overall plans
- A – Recommend disposition policy
- A – Write disposition policy
- A – Test disposition/EDP plan

(6) Identification and Authentication (I&A) Policy

- E – Discuss authentication
- E – Discuss non-repudiation
- E – Define account management

- E – Define authentication
- E – Define biometrics
- E – Define identification and authentication (I&A)
- E – Define non-repudiation
- E – Define peer-to-peer security
- E – Define unauthorized access
- E – Describe how to choose appropriate passwords, and how/why to protect them
- E – Explain need for account management
- E – List underlying account management principles
- E – List underlying authentication principles
- E – List underlying security concerns with password sharing
- E – Discuss good passwords/password conventions
- I – Explain password management/password conventions
- I – Develop authentication schema
- I – Develop local policies and procedures governing password sharing
- I – Develop non-repudiation schema
- I – Develop organizational policies and procedures for password use/selection
- I – Develop security policy for account administration
- I – Discuss account management
- I – Discuss authentication principles
- I – Explain authentication policy
- I – Explain I&A
- I – Explain I&A policy
- I – Explain need for authentication
- I – Explain peer-to-peer security policy
- I – Implement account management
- I – Implement biometrics
- I – Implement non-repudiation schema
- I – Present authentication identification and authentication policy
- I – Propose methods to share files without sharing passwords
- I – Summarize biometrics
- I – Summarize peer-to-peer security policy
- A – Discuss good password systems
- A – Implement authentication
- A – Integrate authentication into local policy
- A – Integrate biometrics into systems
- A – Integrate I&A into overall plans
- A – Integrate peer-to-peer security into local policy
- A – Write authentication policy
- A – Write biometrics policy
- A – Write I&A policy
- A – Write peer-to-peer security policy

(7) Monitoring and Auditing Policy

- E – Define electronic monitoring
- E – Define intrusion detections
- E – Define keystroke monitoring

- E – Define keystroke monitoring requirements for policy and procedures
- E – Define monitoring
- E – Define required audit features
- E – Define requirements for error logs/system logs
- E – Describe audit collection requirements
- E – Describe policy for audit
- E – Identify audit and log tools
- E – Identify error and system tools
- E – Outline known means of electronic monitoring
- E – Outline known means of keystroke monitoring
- I – Develop audit policy
- I – Develop audit trails and logging policy and procedures in compliance with legal requirements
- I – Develop electronic monitoring policy
- I – Develop monitoring techniques and methods
- I – Develop policy and procedures on use of audit trails and logging
- I – Develop policy and procedures on use of error logs/system logs
- I – Develop policy for monitoring and auditing information systems
- I – Discuss audit collection requirements
- I – Discuss audit policy and procedures
- I – Discuss electronic monitoring
- I – Discuss monitoring
- I – Discuss policy and procedures
- I – Implement audit trail and logging
- I – Implement electronic monitoring policy
- I – Implement logging
- I – Implement monitoring policy
- I – Propose implementation of intrusion detection
- I – Use audit collection
- I – Use results of electronic monitoring reports
- A – Discuss audit collection requirements
- A – Write audit trail error logs/system logs
- A – Write audit trail logging policy
- A – Write electronic monitoring policy
- A – Write keystroke monitoring policy
- A – Write monitoring policy
- A – Write policies for intrusion detection in accordance with higher level policies

C. CONTROL SYSTEMS POLICIES

(1) Configuration Management Policy

- E – Define configuration management
- E – Define Configuration Control Board (CCB)
- I – Discuss change controls
- I – Discuss configuration CCB
- I – Integrate change control into operations
- I – Plan change control

- A – Evaluate change control plan
- A – Integrate information system security requirements into configuration management program
- A – Write configuration management policy

(2) Protective Technology Policy

- E – Define protective technology
- E – List protective technologies
- I – Develop policy for integrating protective technology
- A – Explain protective technologies policy
- A – Predict requirements for protective technology policy
- A – Write protective technology policy

(3) Intrusion Detection Policy

- E – Define intrusion detection
- I – Develop policy governing intrusion detection
- I – Discuss intrusion detection policy
- I – Explain intrusion detection policy
- I – Identify requirements for intrusion detection
- A – Write intrusion detection policy

(4) Malicious Code Policy

- E – Define malicious code
- E – Describe malicious code and outline various types of malicious code
- E – Describe techniques for protection from malicious code to users, and provide examples (real and theoretical)
- I – Propose methods and policies to combat introduction of malicious code into system
- A – Explain consequences of introducing malicious code
- A – Integrate protection techniques into policies
- A – Write policy on malicious code

(5) Access Controls

- E – Define need to understand policy
- E – Define need-to-know
- E – Define risk management policy
- E – Explain user access policy
- E – Explain user access requirements
- I – Develop need to understand policy
- I – Develop security policy for administration of access controls
- I – Explain access control requirements
- I – Explain risk management to access control policy
- I – Summarize risk management policy
- A – Integrate access controls into policy
- A – Summarize risk management policy
- A – Write access control policy
- A – Write risk management policy
- A – Write user access policy

D. CULTURE AND ETHICS

(1) Policy

- E – Define culture and ethics policy
- E – Define roles, responsibilities, and organization (e.g., separation of duties)
- E – Identify basic management issues and their impact on information systems security program
- I – Demonstrate professional ethics
- I – Explain professional ethics
- I – Develop policy governing use of information systems
- I – Discuss importance of privacy
- I – Discuss privacy policy
- I – Explain organization’s culture and its affect on security of information systems
- I – Explain privacy policy
- A – Implement privacy policy
- A – Integrate privacy concerns and laws into organizational policy
- A – Write policy governing appropriate use of information system
- A – Write privacy policy

(2) Organization Culture

- E – Describe organization culture
- I – Explain organization culture
- I – Explain organization culture policy

(3) Basic/Generic Management Issues

- E – Describe basic/generic management issues
- A – Integrate management issues into local policy

(4) Agency-Specific Security Policies & Procedures

- E – Describe how effective security policies and procedures can reduce threats to information systems
- E – Identify security policy-making bodies
- I – Write local guidance
- A – Interpret agency policy and procedures for guiding local policy and procedures

E. INCIDENT RESPONSE

(1) Concept of Operations (CONOP)

- E – Define Concept of Operations (CONOP)
- I – Develop CONOP
- I – Develop CONOP policy
- I – Discuss information covered by CONOP
- I – Propose methods and policies to include in CONOP
- A – Integrate standard operating procedures into CONOP
- A – Write CONOP policy

(2) Criminal Activity Preparedness Planning

- E – Explain criminal activity preparedness planning policy
- I – Develop policy for criminal activity
- A – Evaluate criminal activity preparedness plan
- A – Integrate criminal activity preparedness into local policy
- A – Summarize criminal activity preparedness plan
- A – Write policy for criminal activity

(3) Organizational/Agency Systems Emergency/Incident Response Team

- E – Define organizational/agency systems emergency/incident response team
- E – Identify organizational/agency systems emergency/incident response team
- E – Interact with organizational/agency systems emergency/incident response team to resolve incidents

(4) Malicious Code

- E – Define malicious code
- E – Describe malicious code and outline various types of malicious code
- E – Describe techniques for protection from malicious code to users, and provide examples (real and theoretical)
- I – Propose methods and policies to combat introduction of malicious code into system
- A – Integrate protection techniques into policies
- A – Write policy on malicious code

II. IMPLEMENT SITE SECURITY POLICY

A. CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY (CIA)

(1) Contingency Plans

- I – Develop contingency plan
- I – Discuss current contingency plan with necessary parties
- I – Explain contingency plan
- I – Monitor contingency plan training
- I – Propose contingency plan
- I – Summarize contingency plan
- A – Direct implementation of contingency plan
- A – Direct operation of contingency plan
- A – Influence management on importance of having properly trained SA/staff to perform contingency plan on mission critical systems
- A – Test contingency plan
- A – Verify current contingency plan is available and accurate
- A – Verify that necessary parties understand contingency plan and where it is maintained
- A – Write contingency plan

(2) Emergency Destruction Procedures (EDP)

- E – Discuss current emergency destruction plan (EDP) with necessary parties
- I – Develop EDP
- I – Explain EDP
- I – Monitor EDP training
- I – Summarize EDP
- I – Verify that necessary parties understand EDP and where it is maintained
- A – Direct implementation of EDP
- A – Direct operation of EDP
- A – Influence management on importance of having properly trained SA/staff to perform EDP on mission critical systems
- A – Propose EDP
- A – Test EDP
- A – Verify current EDP is available and accurate
- A – Write EDP

(3) Continuity Plans

(a) **Reconstitution**

- I – Discuss current reconstitution plan with necessary parties to ensure they understand their respective reconstitution roles and responsibilities.
- I – Explain reconstitution plan
- I – Explain restoration
- I – Monitor reconstitution plan training
- I – Monitor restoration/reconstitution
- I – Summarize restoration/reconstitution plan

- I – Verify that necessary parties understand restoration/reconstitution plans and where they are maintained
- A – Develop restoration/reconstitution plan
- A – Direct implementation of reconstitution plan
- A – Direct operation of reconstitution plan
- A – Implement and maintain recovery procedures
- A – Implement recovery procedures
- A – Implement testing and assessment
- A – Implement training
- A – Influence management on importance of having properly trained SA/staff to perform reconstitution plan on mission critical systems
- A – Propose reconstitution plan
- A – Test/exercise restoration/reconstitution plan
- A – Verify current restoration/reconstitution plan is available and accurate
- A – Write restoration/reconstitution plan
- A – Evaluate test/execution of reconstitution plan

(b) Recovery

- E – Address recovery procedures with SA/staff
- I – Develop recovery plan
- I – Direct SA/staff to use recovery plan during recovery
- I – Discuss current recovery plan with necessary parties
- I – Explain recovery plan
- I – Monitor recovery plan training
- I – Summarize recovery plan
- I – Verify that necessary parties understand recovery plan and where it is maintained
- A – Direct implementation of recovery plan
- A – Direct operation of recovery plan
- A – Influence management on importance of having properly trained SA/staff to perform recovery plan on mission critical systems
- A – Propose recovery plan
- A – Test recovery plan
- A – Verify current recovery plan is available and accurate
- A – Verify SA understands rules for restoring files
- A – Write recovery plan

(c) Accountability

- E – Define who has responsibility for accountability
- E – Describe accounting process for hardware, software, and information
- E – Outline accountability process/program
- A – Verify assigned responsibilities are commensurate with underlying information system security policies and are appropriately assigned

(4) Disposition of Classified Material

- E – Address disposition procedures with system administrator SA/staff
- E – Explain the maintenance of audit records
- I – Develop disposition plan

- I – Direct SA/staff to review relevant policy and procedures for disposition of classified material
- I – Direct SA/staff to use disposition plan
- I – Discuss current disposition plan with necessary parties
- I – Explain disposition plan
- I – Monitor disposition plan training
- I – Summarize disposition plan
- I – Verify that necessary parties understand disposition plan and where it is maintained
- A – Direct implementation of disposition plan
- A – Direct operation of disposition plan
- A – Influence management of importance of having properly trained SA/staff to perform disposition plan on mission critical systems
- A – Propose disposition plan
- A – Test disposition plan
- A – Verify current disposition plan is available and accurate
- A – Verify disposition classified material plan is executed
- A – Verify SA understands rules to disposition procedures
- A – Write disposition plan
- A – Evaluate disposition plan

(5) Monitoring and Auditing

Alarms, Signals, & Reports

- E – Address auditing and logging management with SA/staff
- E – Address work force auditing and logging management procedures
- E – Discuss alarms, signals, and reports requirements
- E – Discuss auditing and logging management policies, laws, and penalties with personnel
- E – Discuss current auditing and logging management with necessary parties
- I – Develop auditing and logging management plan
- I – Direct SA to follow proper auditing and logging management procedures
- I – Direct SA to implement auditing and logging management procedures
- I – Direct SA/staff to follow proper auditing and logging procedures
- I – Direct SA/staff to follow proper monitoring and auditing procedures
- I – Direct SA/staff to restrict access to auditing and logging functions and collected log files
- I – Direct SA/staff to restrict access to auditing and logging system and collected information
- I – Direct SA/staff to review policy and procedures for auditing and logging management
- I – Direct SA/staff to review relevant policy and procedures for auditing and logging management
- I – Direct SA/staff to use auditing and logging management
- I – Explain alarms, signals, and reports requirements
- I – Explain auditing and logging management plan
- I – Monitor auditing and logging management plan training
- I – Summarize auditing and logging management plan

- I – Use analysis of intrusion indicators, when appropriate, and generate results
- I – Verify that necessary parties understand auditing and logging management plan and where it is maintained
- A – Direct implementation of auditing and logging management plan
- A – Direct operation of auditing and logging management plan
- A – Establish auditing and logging management policy for infractions
- A – Implement auditing and logging management policy
- A – Implement auditing and logging management reporting
- A – Influence management on importance of having properly trained SA/staff to perform auditing and logging management plan on mission critical systems
- A – Interpret legal aspects of logging and auditing systems
- A – Prescribe changes that result from analysis
- A – Prescribe oversight associated with alarms and signals
- A – Propose auditing and logging management plan
- A – Test alarms, signals, and reports
- A – Test auditing and logging management plan
- A – Verify adherence to auditing and logging procedures
- A – Verify auditing and logging management plan is executed
- A – Verify current auditing and logging management plan is available and accurate
- A – Verify monitoring and auditing procedures and that they are being followed
- A – Verify SA understands rules for auditing and logging management
- A – Verify strategic items being audited and logged
- A – Verify strategic placement of auditing and logging system
- A – Write auditing and logging management plan

(6) Audit Trail and Logging, Error/System Logs

- I – Prescribe changes resulting from evaluation alarms, signals, & reports

(7) Intrusion Detection

- E – Address intrusion detection management with SA/staff
- E – Address SA/staff about monitoring and auditing intrusion detection policies
- E – Address work force about intrusion detection management procedures
- I – Develop intrusion detection management plan
- I – Direct implementation of intrusion detection management plan
- I – Direct operation of intrusion detection management plan
- I – Direct SA/staff to follow proper intrusion detection management procedures
- I – Direct SA/staff to implement intrusion detection management procedures
- I – Direct SA/staff to follow proper monitoring and auditing procedures
- I – Direct SA/staff to restrict access to intrusion detection system and collected information
- I – Direct SA/staff to review relevant policy and procedures for intrusion detection management
- I – Direct SA/staff to review relevant policy and procedures for intrusion detection management
- I – Direct SA/staff to use intrusion detection management
- I – Discuss current intrusion detection management plans, policies, and procedures with necessary parties

- I – Discuss intrusion detection management policies, laws, and penalties with personnel
- I – Explain intrusion detection management plan
- I – Monitor intrusion detection management plan training
- I – Summarize intrusion detection management plan
- I – Verify that necessary parties understand intrusion detection management plan and where it is maintained
- A – Establish intrusion detection management policy for infractions
- A – Implement intrusion detection management policy
- A – Implement intrusion detection management reporting
- A – Influence management on importance of having properly trained SA/staff to execute intrusion detection management plans, policies, and procedures on mission critical systems
- A – Interpret legal aspects of intrusion detection systems
- A – Propose intrusion detection management plan
- A – Test intrusion detection management plan
- A – Verify current intrusion detection management plan is available and accurate
- A – Verify intrusion detection management plan is executed
- A – Verify intrusion detection management policy is followed
- A – Verify monitoring and auditing procedures and that they are being followed
- A – Verify SA understands rules for intrusion detection management
- A – Verify strategic placement of intrusion detection system
- A – Write intrusion detection management plan

(8) Investigation of Security Breaches

- E – Define security breaches
- I – Discuss consequences of security breaches
- I – Discuss security breaches
- A – Evaluate results of security breaches
- A – Evaluate significance of security breaches
- A – Implement policy for addressing security breaches
- A – Prescribe changes resulting from evaluation of security breaches
- A – Prescribe oversight associated with investigations
- A – Test security breach detection systems
- A – Verify security breach policy is implemented

(9) Monitoring

- E – Address monitoring management with SA/staff
- E – Address SA/staff about legal monitoring restrictions
- E – Address work force about monitoring management procedures
- I – Develop monitoring management plan
- I – Direct SA/staff to follow proper monitoring management procedures
- I – Direct SA/staff to help work force with monitoring management procedures
- I – Direct SA/staff to follow appropriate laws and policies for monitoring
- I – Direct SA/staff to follow proper monitoring procedures
- I – Direct SA/staff to restrict access to monitoring functions and collected log files
- I – Direct SA/staff to restrict access to monitoring system and collected information

- I – Direct SA/staff to review relevant policy and procedures for monitoring
- I – Direct SA/staff to use monitoring management procedures
- I – Discuss current monitoring management with necessary parties
- I – Discuss monitoring management policies, laws, and penalties with personnel
- I – Explain monitoring management plan
- I – Monitor monitoring management plan training
- I – Summarize monitoring management plan
- I – Verify that necessary parties understand monitoring management plan and where it is maintained
- A – Direct implementation of monitoring management plan
- A – Direct operation of monitoring management plan
- A – Establish policy infractions for monitoring management
- A – Implement monitoring management policy
- A – Implement monitoring management reporting
- A – Influence management on importance of having properly trained SA/staff to perform monitoring management plan on mission critical systems
- A – Interpret legal aspects of monitoring systems
- A – Propose monitoring management plan
- A – Test monitoring management plan
- A – Verify adherence to appropriate laws and policies for monitoring
- A – Verify adherence to monitoring procedures
- A – Verify current monitoring management plan is available and accurate
- A – Verify monitoring and auditing procedures and that they are being followed
- A – Verify monitoring management plan is executed
- A – Verify monitoring management policy is followed
- A – Verify SA understands rules for monitoring management
- A – Verify strategic items being monitored
- A – Verify strategic placement of monitoring systems
- A – Verify that consent to monitoring banners are in place
- A – Verify that process for maintaining signed consent to monitoring forms exists
- A – Write monitoring management plan

(10) Configuration Management

- E – Address configuration management with SA/staff
- E – Address SA/staff about legal configuration restrictions
- E – Address work force about configuration management procedures
- I – Direct SA to follow proper configuration management procedures
- I – Direct SA to help work force with configuration management procedures
- I – Direct SA/staff to follow appropriate laws and policies for configuration
- I – Direct SA/staff to follow configuration control software procedures
- I – Direct SA/staff to follow proper configuration procedures
- I – Direct SA/staff to restrict access to configuration functions and collected log files
- I – Direct SA/staff to restrict access to configuration system and collected information
- I – Direct SA/staff to review relevant policy and procedures for configuration management
- I – Direct SA/staff to use configuration management procedures
- I – Discuss configuration management policies, laws and penalties with personnel

- I – Discuss current configuration management with necessary parties
- I – Explain configuration management plan
- I – Monitor configuration management plan training
- I – Summarize monitoring management plan
- I – Verify that necessary parties understand configuration management plan and where it is maintained
- A – Develop configuration management plan
- A – Direct implementation of configuration management plan
- A – Direct operation of configuration management plan
- A – Establish configuration management policy
- A – Implement configuration management policy
- A – Implement configuration management reporting
- A – Influence management on importance of having properly trained SA/staff to perform configuration management plan on mission critical systems
- A – Interpret legal aspects of configuration systems
- A – Propose configuration management plan
- A – Test configuration management plan
- A – Verify adherence to appropriate laws and policies for configuration procedures
- A – Verify adherence to configuration procedures
- A – Verify configuration and auditing procedures and ensure that they are being followed
- A – Verify configuration management plan is executed
- A – Verify configuration management policy is followed
- A – Verify current configuration management plan is available and accurate
- A – Verify SA understands rules for configuration management
- A – Verify strategic items being under configuration management
- A – Verify that software configuration is restricted
- A – Write configuration management plan

(11) Countermeasures

(a) Intrusion Detection

- E – Discuss intrusion detection problems
- I – Direct intrusion detection be implemented
- I – Explain intrusion detection problems
- A – Evaluate results of intrusion detection process
- A – Prescribe changes resulting from evaluation of intrusion detection process
- A – Prescribe oversight associated with intrusion detection process
- A – Test intrusion detection system
- A – Verify intrusion detection is in accordance with policy

(b) Protective technologies

- E – Define cryptanalytic techniques
- E – Define cryptographic concepts
- E – Define digital signatures/non-repudiation
- E – Define key management
- E – Define message digests (e.g., MD5, SHA, HMAC)
- E – Define methods of encryption
- E – Identify protective technologies

- I – Discuss methods of encryption
- I – Discuss protective technologies implementation
- I – Explain alternatives (e.g., steganography, watermarking)
- I – Explain cryptanalytic techniques
- I – Explain cryptographic concepts
- I – Explain digital signatures/non-repudiation
- I – Explain email security (e.g., PGP, PEM)
- I – Explain internet security (e.g., SSL)
- I – Explain key management
- I – Explain message digests (e.g., MD5, SHA, HMAC)
- I – Explain public key infrastructure (PKI) (e.g., certification authorities, etc)
- I – Present protective technologies implementation plan
- I – Recommend alternatives (e.g., steganography, watermarking)
- I – Recommend digital signatures/non-repudiation tools
- I – Recommend email security (e.g., PGP, PEM)
- I – Recommend internet security (e.g., SSL)
- I – Recommend message digests (e.g., MD5, SHA, HMAC) tools
- I – Recommend protective technologies
- I – Recommend public key infrastructure (PKI) (e.g., certification authorities, etc.)
- I – Summarize protective technologies implementation plan
- A – Plan protective technologies implementation
- A – Test alternatives (e.g., steganography, watermarking)
- A – Test email security (e.g., PGP, PEM)
- A – Test internet security (e.g., SSL)
- A – Test protective technologies plan
- A – Test public key infrastructure (PKI) (e.g., certification authorities, etc.)
- A – Verify countermeasures exist and that countermeasure procedures are being followed
- A – Verify protective technologies performs as expected

B. ENSURE FACILITY IS APPROVED

- E – Define an approved facility
- E – Define an approved service
- I – Explain what constitutes approved facility
- I – Explain what constitutes approved service
- I – Monitor acquisition of approved facility
- I – Monitor acquisition of approved service
- I – Monitor operation of approved facility
- I – Monitor operation of approved service
- I – Present approved facility plan to SSM, viz., CIO, DAA, CTO, etc.
- I – Present approved service plan to SSM, viz., CIO, DAA, CTO, etc.
- I – Recommend approved facility configuration
- I – Summarize major elements of an approved facility
- I – Summarize major elements of an approved service
- A – Direct Contracting Officer's Technical Representative (COTR) through facility acquisition process
- A – Direct COTR through service acquisition process

- A – Evaluate contracted security services
- A – Integrate security services
- A – Plan an approved facility
- A – Plan an approved service
- A – Plan for acquisition of an approved facility
- A – Plan for acquisition of an approved service
- A – Report on contracted security services
- A – Verify facility is approved appropriate authority
- A – Verify service is approved appropriate authority
- A – Write plan for implementing an approved facility
- A – Write plan for implementing an approved service contract

C. OPERATIONS

(1) Security Policy

- I - Ensure Information System is installed, operated, used, maintained, and disposed of in accordance with security policy

(2) Agency/Vendor Cooperation/Coordination

- E – Describe agency policy for redeploying classified systems to the SA and SSM viz., CIO, DAA, CTO, etc.
- E – Explain agency policy for access by uncleared individuals and vendors to the SA and SSM viz., CIO, DAA, CTO, etc.
- E – Explain cooperation concerns to vendors
- E – Explain cooperation concerns with vendors to SSM, viz., CIO, DAA, CTO, etc.
- E – Facilitate agency control of access by uncleared individuals and vendors
- E – Facilitate correct agency redeployment of classified systems
- E – Facilitate vendor cooperation
- I – Present the agency policy for access by uncleared individuals and vendors
- I – Present the agency policy for redeploying classified systems
- I – Present vendor cooperation report
- I – Summarize vendor cooperation
- A – Evaluate agency policy for access by uncleared individuals and vendors
- A – Evaluate agency policy for redeploying classified systems
- A – Evaluate vendor cooperation
- A – Report vendor cooperation
- A – Verify corrective vendor actions when required

(3) Certification Advocacy

- E – Define advocacy
- E – Explain advocacy role
- I – Demonstrate compliance with certification plan
- I – Explain certification to SSM, viz., CIO, DAA, CTO, etc.
- I – Explain certification to SA
- A – Coordinate with certifier

(4) Conduct Risk Assessment

- E – Define information valuation
- E – Define risk assessment

- E – Describe risk assessment process
- E – Describe three states of information
- I – Develop policy and procedures for conducting a risk assessment
- I – Summarize risk profile
- I – Write risk assessment reports
- A – Coordinate resources to perform a risk assessment
- A – Coordinate risk assessment process
- A – Interpret results of a risk assessment
- A – Interpret risk assessment report
- A – Write risk assessment plan
- A – Write risk assessment policy
- A – Analyze threats to and vulnerabilities of an information system

(5) Contracting for Security Services

- E – Define an approved service
- E – Explain security services to contracting officers
- I – Direct contracting officers to incorporate security services as required
- I – Discuss Protection Profiles and Security Target
- I – Explain what constitutes an approved service
- I – Monitor acquisition of approved service
- I – Monitor operation of approved service
- I – Plan an approved service
- I – Plan for acquisition of an approved service
- I – Present approved service plan to SSM, viz., CIO, DAA, CTO, etc.
- I – Summarize major elements of an approved service
- A – Direct COTR through service acquisition process
- A – Evaluate contracted security services
- A – Integrate security services contracts
- A – Report on contracted security services
- A – Verify obligation for security services
- A – Verify service is approved by appropriate authority
- A – Write plan for implementing an approved service contract

(6) Ensure information system is approved

- A – Verify system approval with SSM, viz., CIO, DAA, CTO, etc.

(7) Life Cycle System Security Planning

- E – Define life cycle security
- E – Describe agency policy for redeploying classified systems
- E – Explain life cycle security planning
- E – Explain life cycle system security planning
- I – Explain agency policy for redeploying classified systems
- I – Direct life cycle system security planning
- I – Direct SA to incorporate life cycle security planning as required
- I – Explain life cycle security plan
- I – Monitor life cycle security acquisition process
- I – Monitor life cycle security process
- I – Plan life cycle security

- I – Present life cycle security plan to SSM, viz., CIO, DAA, CTO, etc.
- I – Summarize major elements of life cycle security
- A – Evaluate life cycle security implementation
- A – Implement Data Item Descriptions (DID) for life cycle security
- A – Implement life cycle security process to support CONOPS
- A – Integrate life cycle security
- A – Report on life cycle security implementation
- A – Validate use of appropriate life cycle security process
- A – Verify life cycle security planning is approved
- A – Verify life cycle system security planning is implemented

(8) System Security Architecture Study

- E – Address system security architecture study
- E – Define system security architecture
- E – Explain system security architecture study
- I – Direct SA to incorporate system security architecture study as required
- I – Direct support of system security architecture
- I – Direct system security architecture study
- I – Explain system security architecture study
- I – Monitor system security architecture acquisition process
- I – Monitor system security architecture process
- I – Present system security architecture study to SSM, viz., CIO, DAA, CTO, etc.
- I – Summarize major elements of system security architecture
- A – Evaluate system security architecture implementation
- A – Implement DIDS for system security architecture
- A – Integrate system security architecture
- A – Report on system security architecture implementation
- A – Study system security architecture
- A – Validate appropriate system security architecture process
- A – Verify results mapped to security CONOPS
- A – Verify that security architecture study provides for defense in depth
- A – Verify system security architecture is approved
- A – Verify system security architecture study is implemented

D. GENERAL PRINCIPLES

(1) Access Control Models

- E – Discuss access control models

(2) Approval to Operate

- E – Explain approval to operate
- A – Verify SSM, viz., CIO, DAA, CTO, etc. can discuss approval to operate

(3) Attack

- E – Explain attack
- E – Explain backdoor routines
- E – Explain denial-of-service (DOS) attacks
- E – Explain remote explorer attack

- E – Explain attack root exploits
- E – Explain session hijacking tools
- E – Explain war dialer/THC-scan attacks
- E – Explain war dialers

(4) Business Aspects of Information Security

- E – Explain business aspects of information security

(5) Common Criteria

- I – Discuss common criteria
- I – Explain common criteria
- I – Discuss Evaluation Assurance Levels (EALs)
- I – Summarize common criteria
- A – Verify security services as defined by common criteria are implemented

(6) Computer Network Attack

- E – Explain computer network attack

(7) Criminal Prosecution

- E – Explain criminal prosecution

(8) Defense in Depth

- E – Give examples of defense in depth methods
- I – Discuss defense in depth
- I – Explain defense in depth
- I – Explain the role of vendors and uncleared individuals in defense in depth
- I – Explain the Model for Information Assurance: An Integrated Approach (2nd Annual IEEE Systems, Man and Cybernetics Information Assurance Workshop, June 2002)
- I – Summarize defense in depth
- A – Verify implementation of defense in depth
- A – Verify security architecture provides defense in depth

(9) Due Care

- E – Address questions from users about due care
- E – Monitor adherence to due care rules
- E – Remind users of due care rules
- I – Explain generally accepted systems security principles (GASSP)
- I – Identify standards upon which GASSP are based
- A – Integrate GASSP into standard operating procedures
- A – Interpret due care rules
- A – Verify due care concerns are addressed
- A – Verify GASSP is implemented
- A – Verify implementation of due care rules
- A – Report to management and SA of status of due care rules
- A – Report on GASSP implementation
- A – Report violations of due care rules

(10) Education, Training, & Awareness

- E – List topics for inclusion into education, training and awareness plan
- E – Recognize AT&E is a countermeasure
- I – Develop education, training, and awareness plan

(11) Industrial Security

- E – Explain industrial security

(12) Information Warfare (INFOWAR) Concepts

- E – Explain INFOWAR concepts
- A – Discuss INFOWAR

(13) Intellectual Property Rights

- E – Explain intellectual property rights
- A – Verify SSM, viz., CIO, DAA, CTO, etc. understands intellectual property rights

(14) Interim Approval to Operate (IATO)

- E – Explain interim approval to operate
- A – Verify SSM, viz., CIO, DAA, CTO, etc. can discuss IATO

(15) Investigative Authorities

- E – Explain investigative authorities
- A – Verify SSM, viz., CIO, DAA, CTO, etc. can discuss investigative authorities

(16) Knowledge of Security Laws*

- E – Discuss Clinger-Cohen Act
- E – Discuss Computer Fraud and Abuse Act
- E – Discuss Computer Security Act
- E – Discuss Copyright Law of the United States and related laws
- E – Discuss Copyright protection and licenses
- E – Discuss Electronic Freedom of Information Act
- E – Discuss Electronic Records Management and Federal Records Act
- E – Discuss Federal Information System Management Act
- E – Discuss Federal Managers Financial Integrity Act
- E – Discuss Federal Property and Administration Service Act
- E – Discuss Freedom of Information Act
- E – Discuss Government Paperwork Elimination Act/Paperwork Reduction Act
- E – Discuss Government Information Security Reform Act
- E – Discuss Millennium Copyright Act
- E – Discuss National Archives and Records Act
- E – Discuss Privacy Act/Privacy Act issues
- E – Discuss USA Patriot Act
- E – Discuss computer crime and the various methods
- E – Discuss international legal issues which can affect Information Assurance
- E – Discuss the legal responsibilities of the SSM, viz., CIO, DAA, CTO, etc.

* As amended

(17) Lattice Model

- E – Define lattice model

(18) Law Enforcement Interfaces

- E – Explain law enforcement interfaces
- A – Discuss law enforcement Interfaces

(19) Multi-level Security

- I – Discuss access control models

(20) Need for System Certification

- E – Explain need for system certification
- A – Verify SSM, viz., CIO, DAA, CTO, etc. can discuss system certification requirements and processes

(21) Operating Security Features

- E – Explain operating security features

(22) Risk Management

- E – Explain risk management
- I – Explain risks associated with agency policy for access by uncleared individuals and vendors
- I – Explain risks associated with agency policy for redeploying classified systems
- A – Discuss risk management

(23) Security Awareness as a countermeasure

- E – Define security awareness for information system users
- I – Develop security awareness plan and materials for information system users
- I – Discuss requirements for security awareness

(24) Security Education as a countermeasure

- E – Encourage employees to seek education in IA as a countermeasure
- I – Discuss security education
- I – Monitor changing security education requirements for information system users
- A – Develop/design information system education programs

(25) Security Training as a countermeasure

- E – Define security training for information system users
- I – Develop security training plan and materials for information system users
- I – Discuss requirements for security training

(26) Software Licensing

- E – Explain software licensing
- A – Discuss software licensing

(27) Software Piracy

- E – Explain software piracy
- A – Discuss software piracy

(28) Systems Security Authorization Agreement (SSAA)

- E – Explain SSAA
- A – Discuss SSAA

(29) Systems Security Plan (SSP)

- E – Explain Systems Security Plan (SSP)
- A – Discuss SSP

(30) Standards of Conduct

- E – Explain standards of conduct

(31) ITSEC/Common Criteria

- I – Discuss ITSEC/Common Criteria

(32) Waive Policy to Continue Operation

- E – Explain Waive Policy to Continue Operation
- A – Discuss Waive Policy to Continue Operation

E. SECURITY MANAGEMENT**(1) Electronic Records Management**

- E – Define electronic records management program and tools
- E – Define underlying rules for electronic records management program
- E – Describe the effect of electronic records management on the system
- I – Explain electronic records management
- I – Monitor electronic records management system
- A – Verify implementation of records management program

(2) Records Retention

- E – Discuss electronic records retention program
- E – Define underlying rules for electronic records retention program
- E – Describe effect of records retention system
- E – List use of record retention
- I – Monitor records retention program

(3) E-Mail

- E – Address SA/staff about legal e-mail monitoring restrictions
- E – Describe e-mail retention policies as they apply to system
- E – Describe e-mail system/e-mail system security
- E – Describe e-mail system and its potential vulnerabilities
- E – Explain e-mail monitoring management with SA/staff
- I – Develop e-mail monitoring management plan
- I – Direct implementation of e-mail monitoring management plan
- I – Direct operation of e-mail monitoring management plan
- I – Direct SA to follow proper e-mail monitoring management procedures
- I – Direct SA to help work force with e-mail monitoring management procedures
- I – Direct SA/staff to follow appropriate laws and policies for e-mail monitoring
- I – Direct SA/staff to follow proper e-mail monitoring procedures
- I – Direct SA/staff to restrict access to e-mail monitoring functions and collected log files
- I – Direct SA/staff to restrict access to e-mail monitoring system and collected information

- I – Direct SA/staff to review relevant policy and procedures for e-mail monitoring management
- I – Direct SA/staff to use e-mail monitoring management procedures
- I – Discuss current e-mail monitoring management with necessary parties
- I – Discuss e-mail monitoring management policies, laws, and penalties with personnel
- I – Explain monitoring management plan
- I – Monitor e-mail monitoring management plan training
- I – Summarize e-mail monitoring management plan
- I – Verify that necessary parties understand e-mail monitoring management plan and where it is maintained
- A – Establish e-mail monitoring management policy for infractions
- A – Implement e-mail monitoring management policy
- A – Implement e-mail monitoring management reporting
- A – Influence management on importance of having properly trained SA/staff to perform e-mail monitoring management plan on mission critical systems
- A – Interpret legal aspects of e-mail monitoring systems
- A – Propose e-mail monitoring management plan
- A – Test e-mail monitoring management plan
- A – Verify adherence to appropriate laws and policies for e-mail monitoring
- E – Discuss appropriate laws and policies for e-mail monitoring
- A – Verify adherence to e-mail monitoring procedures
- A – Verify current e-mail monitoring management plan is available and accurate
- A – Verify e-mail monitoring and auditing procedures and that they are being followed
- A – Verify e-mail monitoring management plan is executed
- A – Verify e-mail monitoring management policy is followed
- A – Verify SA understands rules for e-mail monitoring management
- A – Verify that a process for maintaining signed consent to monitoring forms exists
- A – Verify that consent to monitoring banners are in place
- A – Write e-mail monitoring management plan

(4) Non-Repudiation

- E – Describe non-repudiation and its application to system
- I – Explain non-repudiation
- A – Verify non-repudiation is enforced
- A – Verify non-repudiation is implemented

(5) Hardware Asset Management

- E – Describe agency policy for access by uncleared individuals and vendors
- E – Describe agency policy for redeploying classified systems
- E – Describe hardware asset management program
- E – Describe hardware asset management program and how it applies and is used on the system
- I – Explain agency policy for access by uncleared individuals and vendors
- I – Explain agency policy for redeploying classified systems
- I – Propose hardware asset management process

A – Verify hardware accountability is performed at all levels

A – Verify reconstitution planning is implemented

(6) Software Asset Management

E – Describe agency policy for access by uncleared individuals and vendors

E – Describe agency policy for redeploying classified systems

E – Describe software asset management program

E – Describe software asset management program and how it applies and is used on the system

E – Describe software asset management program and how it applies/is used on system with emphasis on license and copyright issues, and cross reference to ethics

I – Enforce policies and procedures

I – Explain agency policy for access by uncleared individuals and vendors

I – Explain agency policy for redeploying classified systems

I – Promote compliance

A – Propose software asset management process

A – Report non-compliance

A – Verify software accountability is performed at all levels

A – Verify reconstitution planning is implemented

F. ACCESS CONTROLS

(1) Human Access

Require users and system support personnel to have required security clearances, authorizations and need-to-know; indoctrinate before granting access.

(a) Access Authorization

E – Address access management with SA/staff

E – Address SA/staff about legal access restrictions

E – Address work force about access management procedures

E – Describe agency policy for access by uncleared individuals and vendors

E – Address access management with SA/staff

E – Address SA/staff about legal access restrictions

E – Address work force about access management procedures

I – Develop access authorization processes plan

I – Develop access management plan

I – Direct implementation of access management plan

I – Direct operation of access management plan

I – Direct SA to follow proper access management procedures

I – Direct SA to help work force with access management procedures

I – Direct SA/staff to follow access control access procedures

I – Direct SA/staff to follow appropriate laws and policies

I – Direct SA/staff to follow proper access procedures

I – Direct SA/staff to restrict access to access system and collected information

I – Direct SA/staff to restrict access to access functions and collected log files

I – Direct SA/staff to review relevant policy and procedures for access management

I – Direct SA/staff to use access management procedures

- I – Discuss access management policies, laws, and penalties with personnel
- I – Discuss current access management with necessary parties
- I – Develop access authorization processes plan
- I – Develop access management plan
- I – Direct implementation of access management plan
- I – Direct operation of access management plan
- I – Direct SA to follow proper access management procedures
- I – Direct SA to help work force with access management procedures
- I – Direct SA/staff to follow access control access procedures
- I – Direct SA/staff to follow appropriate laws and policies
- I – Direct SA/staff to follow proper access procedures
- I – Direct SA/staff to restrict access to access functions and collected log files
- I – Direct SA/staff to restrict access to access system and collected information
- I – Direct SA/staff to review relevant policy and procedures for access management
- I – Direct SA/staff to use access management procedures
- I – Discuss access management policies, laws and penalties with personnel
- I – Discuss current access management with necessary parties
- I – Explain access authorization processes
- I – Explain access management plan
- I – Explain agency policy for access by uncleared individuals and vendors
- I – Monitor access management plan training
- I – Propose access management plan
- I – Summarize monitoring management plan
- I – Verify that necessary parties understand access management plan and where it is maintained
- A – Establish access management policy for infractions
- A – Implement access management policy
- A – Implement access management reporting
- A – Influence management on importance of having properly trained SA/staff to perform access management plan on mission critical systems
- A – Interpret legal aspects of access systems
- A – Revise policy document
- A – Test access management plan
- A – Verify access and auditing procedures and that they are being followed
- A – Verify access authorization processes are implemented
- A – Verify access management plan is executed
- A – Verify access management policy is followed
- A – Verify adherence to access procedures
- A – Verify adherence to appropriate laws and policies access
- A – Verify current access management plan is available and accurate
- A – Verify SA understands rules for access management
- A – Verify strategic items being under access management
- A – Verify strategic placement of access systems
- A – Verify that consent to access banners are in place
- A – Write access management plan

(b) Access Control Software

- E – Address access control software management with SA/staff
- E – Address SA/staff about legal access restrictions
- E – Address work force about access control software management procedures
- E – Discuss access control software management policies, laws and penalties with personnel
- E – Discuss current access control software management with necessary parties
- I – Develop access control software management plan
- I – Direct SA to follow proper access control software management procedures
- I – Direct SA to help work force with access control software management procedures
- I – Direct SA/staff to follow access control procedures
- I – Direct SA/staff to follow appropriate laws and policies for access control software
- I – Direct SA/staff to follow proper access control software procedures
- I – Direct SA/staff to restrict access control software to access control software system and collected information
- I – Direct SA/staff to restrict access control software to access control software functions and collected log files
- I – Direct SA/staff to review relevant policy and procedures for access control software management
- I – Direct SA/staff to use access control software management procedures
- I – Explain access control software management plan
- I – Monitor access control software management plan training
- I – Summarize monitoring management plan
- I – Verify that necessary parties understand access control software management plan and where it is maintained
- A – Direct implementation of access control software management plan
- A – Direct operation of access control software management plan
- A – Establish access control software management policy for infractions
- A – Implement access control software management policy
- A – Implement access control software management reporting
- A – Influence management on importance of having properly trained SA/staff to perform access control software management plan on mission critical systems
- A – Interpret legal aspects of access control software systems
- A – Propose access control software management plan
- A – Revise policy document
- A – Test access control software management plan
- A – Verify access control software and auditing procedures and that they are being followed
- A – Verify access control software management plan is executed
- A – Verify access control software management policy is followed
- A – Verify adherence to access control software procedures
- A – Verify adherence to appropriate laws and policies for access procedures
- A – Verify current access control software management plan is available and accurate
- A – Verify SA understands rules for access control software management
- A – Verify strategic items being under access control software management

- A – Verify strategic placement of access control software systems
- A – Verify that access to access control software is restricted
- A – Write access control software management plan

(c) Account Management

- E – Address account management with SA/staff
- E – Address work force about account management procedures
- I – Develop account management plan
- I – Direct SA to follow proper account management procedures
- I – Direct SA to help work force with account management procedures
- I – Direct SA/staff to review relevant policy and procedures for account management
- I – Direct SA/staff to use account management
- I – Discuss account management policies, laws, and penalties with personnel
- I – Discuss current account management with necessary parties
- I – Explain account management plan
- I – Monitor account management plan training
- I – Revise policy document
- I – Summarize account management plan
- I – Verify that necessary parties understand account management plan and where it is maintained
- A – Direct implementation of account management plan
- A – Direct operation of account management plan
- A – Establish account management policy for infractions
- A – Implement account management policy
- A – Implement account management reporting
- A – Influence management on importance of having properly trained SA/staff to perform account management plan on mission critical systems
- A – Propose account management plan
- A – Revise policy document
- A – Test account management plan
- A – Verify account management plan is executed
- A – Verify account management policy is followed
- A – Verify current account management plan is available and accurate
- A – Verify system administrator (SA) understands rules for account management
- A – Write account management plan

(d) Authentication Policy

- E – Address authentication with SA/staff
- E – Address work force about authentication procedures
- E – Discuss authentication policies, laws, and penalties with personnel
- E – Discuss current authentication with necessary parties
- I – Develop authentication plan
- I – Direct SA to follow proper authentication procedures
- I – Direct SA to help work force with authentication procedures
- I – Direct SA/staff to review policy and procedures for authentication
- I – Direct SA/staff to use authentication
- I – Explain authentication plan
- I – Monitor authentication plan training

- I – Summarize authentication plan
- I – Verify that necessary parties understand authentication plan and where it is maintained
- A – Direct implementation of authentication plan
- A – Direct operation of authentication plan
- A – Establish authentication policy for infractions
- A – Implement authentication policy
- A – Implement authentication reporting
- A – Influence management on importance of having properly trained SA/staff to perform authentication plan on mission critical systems
- A – Propose authentication plan
- A – Revise policy document
- A – Test authentication plan
- A – Verify authentication plan is executed
- A – Verify authentication policy is followed
- A – Verify current authentication plan is available and accurate
- A – Verify SA understands rules for authentication
- A – Write authentication plan

(e) Biometric Access Management

- E – Address biometric access management with SA/staff
- E – Discuss biometric access management policies, laws and penalties with personnel
- E – Discuss current biometric access management with necessary parties
- I – Develop biometric access management plan
- I – Direct SA/staff to review relevant policy and procedures for biometric access
- I – Direct SA/staff to use biometric access management techniques
- I – Explain biometric access management plan
- I – Monitor biometric access management plan training
- I – Summarize biometric access management plan
- I – Verify that necessary parties understand biometric access management plan and where it is maintained
- A – Direct implementation of biometric access management plan
- A – Direct operation of biometric access management plan
- A – Implement biometric access incident notification policy
- A – Implement biometric access incident reporting
- A – Influence management on importance of having properly trained SA/staff to perform biometric access management plan on mission critical systems
- A – Propose biometric access management plan
- A – Test biometric access management plan
- A – Verify biometric access plan is executed
- A – Verify current biometric access management plan is available and accurate
- A – Verify SA understands rules for biometric access management
- A – Write biometric access management plan

(f) Clearance Verification

- I – Develop clearance policy
- A – Revise policy document
- A – Verify clearance policy is implemented

(g) Need-to-Know Controls

- I – Develop policy for need-to-know controls implementation
- A – Revise policy document
- A – Verify need-to-know controls are implemented

(h) Password Management

- E – Address password management with SA/staff
- E – Address work force authentication procedures
- E – Discuss current password management with necessary parties
- E – Discuss password management policies, laws, and penalties with personnel
- I – Direct SA to follow proper authentication procedures
- I – Direct SA to help work force with authentication procedures
- I – Direct SA/staff to review policy and procedures for password
- I – Direct SA/staff to review relevant policy and procedures for passwords
- I – Direct SA/staff to use password management
- I – Explain password management plan
- I – Monitor password management plan training
- I – Summarize password management plan
- I – Verify that necessary parties understand password management plan and where it is maintained
- A – Develop password management plan
- A – Direct implementation of password management plan
- A – Direct operation of password management plan
- A – Establish policy for password infractions
- A – Implement password incident notification policy
- A – Implement password incident reporting
- A – Influence management on importance of having properly trained SA/staff to perform password management plan on mission critical systems
- A – Propose password management plan
- A – Revise policy document
- A – Test password management plan
- A – Verify authentication policy is followed
- A – Verify current password management plan is available and accurate
- A – Verify password plan is executed
- A – Verify SA understands rules for password management
- A – Write password management plan

(i) Roles and Responsibilities (RBAC – Role Based Access Control)

- I – Develop roles, responsibilities, and access controls policy
- I – Explain roles, responsibilities, and access controls
- A – Revise policy document
- A – Verify roles, responsibilities and access controls are implemented

(j) Unauthorized Access

- E – Address unauthorized access incident reporting with SA/staff
- E – Discuss unauthorized access policies, laws, and penalties with personnel
- I – Develop unauthorized access incident reporting plan
- I – Direct implementation of unauthorized access incident reporting plan
- I – Direct operation of incident reporting plan

- I – Direct SA/staff to review relevant policy and procedures for unauthorized access
- I – Direct SA/staff to review relevant policy and procedures for unauthorized access incident reporting
- I – Direct SA/staff to use incident reporting
- I – Discuss current incident reporting plan with necessary parties
- I – Explain unauthorized access incident reporting plan
- I – Monitor incident reporting plan training
- I – Summarize unauthorized access incident reporting plan
- I – Verify that necessary parties understand unauthorized access incident reporting plan and where it is maintained
- A – Establish policy for unauthorized access infractions
- A – Implement unauthorized access incident reporting
- A – Implement unauthorized access notification policy
- A – Influence management on importance of having properly trained SA/staff to perform unauthorized access incident reporting plan on mission critical systems
- A – Propose incident reporting plan
- A – Revise policy document
- A – Test incident reporting plan
- A – Verify current unauthorized access incident reporting plan is available and accurate
- A – Verify SA understands rules for unauthorized access incident reporting
- A – Verify unauthorized access incident reporting plan is executed
- A – Write incident reporting plan

(2) Key Management

(a) COMSEC

- E – Explain to users and managers what COMSEC process is and how COMSEC process is relevant to them
- E – Identify COMSEC
- E – Identify use for COMSEC material on system
- E – Integrate services and advice of COMSEC Manager (Custodian) with operations
- E – List national COMSEC policies
- E – List national COMSEC procedures
- I – Explain COMSEC policies and their relevance to users
- I – Explain COMSEC policies and their relevance to SA
- I – Explain COMSEC policies and their relevance to SSM, viz., CIO, DAA, CTO, etc.
- I – Summarize COMSEC process
- A – Report on COMSEC process
- A – Review local COMSEC policies and procedures from an information assurance standpoint
- A – Revise local policy document IAW national policies

(b) Key Certificate Administration (EKMS)

- E – Define EKMS
- E – Demonstrate knowledge of how to operate an EKMS system
- E – Describe to users and managers what EKMS is, and how/why it is used

- E – Describe to users and managers what key management is, and how/why EKMS is used
- E – Identify components of EKMS as it applies to system
- E – Identify EKMS requirements
- E – Outline EKMS national policies and procedures and explain their relevance to users
- E – Outline EKMS policies and procedures and explain their relevance to users
- E – Outline national & agency EKMS management policies and procedures, and explain their relevance to users
- E – Submit EKMS requirements
- E – Use EKMS management in a system
- I – Describe EKMS methodology
- I – Design specific EKMS procedures for system in line with policies
- I – Discuss EKMS
- I – Explain EKMS
- I – Prepare EKMS operating procedures for a system
- I – Recommend approved EKMS technology
- I – Use appropriate EKMS system
- A – Compare differing public EKMS methodologies
- A – Evaluate EKMS process for a system
- A – Integrate EKMS management into overall system and procedures
- A – Manage EKMS certificates
- A – Report on EKMS implementation
- A – Resolve EKMS conflict with procedures and policies, and variances thereof
- A – Revise policy document
- A – Verify EKMS procedures are in line with policy
- A – Verify EKMS supports security management requirements
- A – Verify implementation of EKMS

(c) Key Escrow

- E – Describe to users and managers what key escrow is, and how/why it is used
- E – Explain national key escrow policies and procedures
- E – Use key escrow management in a system
- A – Revise policy document IAW national policies
- A – Verify key escrow procedures are in line with policy

(d) KMI

- E – Define KMI
- I – Discuss KMI
- A – Report on KMI implementation

(e) Peer-to-Peer Security

- E – Define peer-to-peer
- E – Identify peer-to-peer requirements
- I – Discuss peer-to-peer
- I – Explain peer-to-peer
- I – Submit peer-to-peer requirements
- A – Report on peer-to-peer implementation
- A – Revise policy document

- A – Verify implementation of peer-to-peer
- A – Verify peer-to-peer security concerns are addressed

(f) Public Key Infrastructure (PKI)

- E – Define Public Key Infrastructure (PKI)
- E – Demonstrate knowledge of how to operate a PKI system
- E – Describe to users and managers what key management is, and how/why PKI is used
- E – Describe to users and managers what PKI is, and how/why it is used
- E – Identify components of PKI as it applies to system
- E – Identify PKI requirements
- E – Outline national & agency PKI management policies and procedures, and explain their relevance to users
- E – Outline PKI national policies and procedures and explain their relevance to users
- E – Outline PKI policies and procedures and explain their relevance to users
- E – Submit PKI requirements
- E – Use PKI management in a system
- I – Describe PKI methodology
- I – Design specific PKI procedures for system IAW national/local policies
- I – Discuss PKI
- I – Explain PKI
- I – Manage PKI Certificates
- I – Prepare PKI operating procedures for a system
- I – Recommend approved PKI technology
- I – Use appropriate PKI system
- A – Compare differing public PKI methodologies
- A – Evaluate PKI process for a system
- A – Integrate PKI management into overall system and procedures
- A – Report on PKI implementation
- A – Resolve PKI conflict with procedures and policies, and variances thereof
- A – Revise policy document
- A – Verify implementation of PKI
- A – Verify PKI procedures are in line with policy
- A – Verify PKI supports security management requirements

G. INCIDENT RESPONSE

Security Investigation Procedures

- E – Assist in investigations as requested
- E – Describe process of investigating security incident
- E – Follow procedures
- E – Identify investigating authorities
- I – Explain procedures to users and managers, significance of actions, and consequences for variations
- I – Monitor compliance with procedure
- I – Propose changes to procedures
- I – Recommend training to avoid incident
- A – Modify SSAA to reflect changes to mediate impact of incident
- A – Review SA response

- A – Review SSAA in light of incident
- A – Verify higher authority/organizational/agency systems emergency/incident response team notification
- A – Verify incident is reported
- A – Verify remediation is executed

3. ENFORCE AND VERIFY SYSTEM SECURITY POLICY

A. CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY/ACCOUNTABILITY (CIA)

(1) *Planning*

(a) Continuity Plans

- E – Discuss continuity plans
- I – Develop continuity plan
- I – Enforce continuity plan
- I – Explain continuity plans
- A – Evaluate results of test of continuity plan
- A – Prescribe changes resulting from evaluation of continuity plan
- A – Prescribe oversight of continuity plans
- A – Propose plan changes
- A – Test continuity plan
- A – Verify continuity plans are implemented
- A – Verify continuity plans are reflected in SSAA
- A – Verify items in continuity plan are in force
- A – Evaluate execution of continuity plan
- A – Evaluate execution of contingency plan

(b) Contingency Plans

- E – Discuss contingency plans
- I – Enforce contingency plan
- I – Explain contingency plan
- I – Develop contingency plan
- I – Summarize contingency plan
- A – Propose plan changes
- A – Verify contingency plans are implemented
- A – Verify items in contingency plan are in force
- A – Prescribe oversight of contingency plans
- A – Evaluate results of test of contingency plan
- A – Test contingency plan
- A – Verify contingency plan test results
- A – Prescribe changes resulting from evaluation of contingency plan
- A – Verify contingency plans are reflected in SSAA

(c) Reconstitution

- E – Discuss reconstitution plans
- I – Enforce reconstitution plan
- I – Explain reconstitution plans
- I – Develop reconstitution plan
- A – Verify reconstitution plans are implemented
- A – Verify items in reconstitution plan are in force
- A – Propose plan changes

- A – Prescribe oversight of reconstitution plans
- A – Evaluate results of test of reconstitution plan
- A – Test reconstitution plan
- A – Prescribe changes resulting from evaluation of reconstitution plan
- A – Verify reconstitution plans are reflected in SSAA
- A – Evaluate reconstitution plan

(d) Disposition of Classified Material & Emergency Destruction Procedures (EDP)

- E – Discuss disposition of classified material & EDP
- I – Explain disposition of classified material & EDP
- I – Enforce disposition of classified material & EDP
- A – Prescribe oversight of disposition of classified material & EDP
- A – Perform EDP
- A – Evaluate results of test of EDP
- A – Propose plan changes
- A – Prescribe changes resulting from evaluation
- A – Evaluate and test disposition of classified material and EDP

(e) Recovery

- I – Summarize recovery plan
- A – Verify recovery plan test results
- A – Verify recovery plans are implemented

(f) Accountability

- A – Verify individuals understand their accountability

(2) Monitoring and Auditing

(a) Alarms, Signals, & Reports

- E – Discuss alarms, signals, and reports requirements
- I – Enforce alarms, signals, and reports requirements
- I – Explain alarms, signals, and reports requirements
- I – Use analysis of intrusion indicators, when appropriate, and generate results
- A – Prescribe changes that result from analysis
- A – Prescribe oversight associated with alarms and signals
- A – Prescribe changes resulting from evaluation alarms, signals, & reports
- A – Test alarms, signals, and reports

(b) Intrusion Detection

- E – Discuss intrusion detection problems
- I – Direct intrusion detection enforced
- I – Enforce intrusion detection requirements
- I – Explain intrusion detection problems
- A – Prescribe oversight associated with intrusion detection process
- A – Test intrusion detection system
- A – Verify intrusion detection is in accordance with policy

(c) Intrusion Deterrents

- A – Verify SA/staff monitors intrusion deterrents status
- A – Verify intrusion deterrents are current, operational, and tested
- A – Verify intrusion deterrents are implemented and enforced

(d) Investigation of Security Breaches

- E – Discuss security breaches
- E – Define security breach
- I – Discuss security breaches
- I – Enforce requirements associated with investigations
- I – Evaluate significance of security breaches
- A – Evaluate results of security breaches
- A – Implement policy for security breach
- A – Prescribe changes resulting from evaluation of security breaches
- A – Prescribe oversight associated with investigations
- A – Test security breach detection systems
- A – Verify security breach policy is implemented

(e) Monitoring

- E – Define keystroke monitoring
- E – Ensure legal requirements for monitoring are enforced
- E – Identify potential monitoring problems
- I – Discuss monitoring management policies, laws, and penalties with personnel
- I – Enforce keystroke monitoring policy
- I – Explain monitoring
- I – Review reports of monitoring events
- I – Explain consequences of unapproved monitoring
- A – Implement monitoring policy
- A – Prescribe changes that were identified as problems
- A – Verify strategic items being monitored
- A – Verify that consent to monitoring banners are in place
- A – Verify that process for maintaining signed consent to monitoring forms exists

(f) Network Monitoring

- E – Discuss network monitoring problems
- E – Explain consequences of unapproved monitoring
- I – Direct network monitoring
- I – Enforce network monitoring requirements
- I – Explain network monitoring problems
- A – Evaluate results of network monitoring process
- A – Prescribe changes resulting from evaluation of network monitoring process
- A – Prescribe oversight associated with monitoring process
- A – Test network monitoring system
- A – Verify network monitoring is in accordance with policy

(3) Environmental Controls

- E – Discuss environmental control issues
- I – Direct environmental control testing as required
- I – Explain environmental control requirements
- A – Evaluate results from environmental control testing
- A – Prescribe changes resulting from evaluation environmental control testing
- A – Prescribe oversight associated environmental controls
- A – Verify environmental control requirements are enforced

(4) Filtered Power

- E – Discuss filtered power issues
- I – Direct filtered power testing as required
- I – Explain filtered power requirements
- A – Evaluate results from filtered power testing
- A – Prescribe changes resulting from evaluation of filtered power testing
- A – Prescribe oversight associated filtered power
- A – Verify filtered power requirements are enforced

(5) Fire Prevention

- E – Discuss fire prevention issues
- I – Direct fire prevention testing as required
- I – Explain fire prevention requirements
- A – Evaluate results from fire prevention testing
- A – Prescribe changes resulting from evaluation of fire prevention testing
- A – Prescribe oversight associated fire prevention
- A – Verify fire prevention requirements are enforced

(6) Grounding

- E – Discuss grounding issues
- I – Direct grounding testing as required
- I – Explain grounding requirements
- A – Evaluate results from grounding testing
- A – Prescribe changes resulting from evaluation of grounding testing
- A – Prescribe oversight associated grounding
- A – Verify grounding requirements are enforced

(7) Safety

- E – Discuss safety issues
- I – Direct safety testing as required
- I – Explain safety requirements
- A – Evaluate results from safety testing
- A – Prescribe changes resulting from evaluation of safety testing
- A – Prescribe oversight associated safety
- A – Verify safety requirements are enforced

B. SECURITY MANAGEMENT**(1) Electronic Records Management**

- A – Verify electronic records management system is operated in accordance with policy
- A – Verify implementation of records management program and describe effect on system

(2) Records Retention

- I – Monitor records retention program
- A – Verify electronic records retention management system is operated in accordance with policy

A – Verify implementation of records retention program and describe effect on system

(3) E-Mail

I – Monitor e-mail program

A – Verify e-mail system is operated in accordance with policy

A – Verify implementation of e-mail system and describe effect on system

A – Verify that privacy laws are enforced

(4) Non-Repudiation

A – Verify implementation of non-repudiation

(5) Hardware Asset Management

A – Verify hardware asset accountability is enforced at all levels

(6) Software Asset Management

A – Verify software asset accountability is enforced at all levels

C. ACCESS CONTROLS

(1) Human Access

Require users and system support personnel to have required security clearances, authorizations and need-to-know, and are indoctrinated before granting access

E – Describe agency policy for access by uncleared individuals and vendors

I – Explain agency policy for access by uncleared individuals and vendors

(a) Access Authorization

A – Revise access authorization policy document

A – Verify access authorization policy is integrated into overall system and procedures

A – Verify access authorization procedures are enforced

(b) Access Control Software

A – Revise access control software policy document

A – Verify access control software policy is integrated into overall system and procedures

A – Verify access control software procedures are enforced

(c) Account Administration

E – Verify requested access

I – Direct account administration tests

I – Enforce account administration policy

A – Prescribe oversight associated with account administration tests

A – Revise account management policy document

A – Verify account management policy is integrated into overall system and procedures

A – Verify account management security procedures are enforced

(d) Authentication Policy

A – Revise authentication policy document

A – Verify authentication policy is integrated into overall system and procedures

A – Verify authentication procedures are enforced

(e) Biometric Access Management

- A – Revise biometric access management policy document
- A – Verify biometric access management policy is integrated into overall system and procedures
- A – Verify biometric access management procedures are enforced
- A – Prescribe oversight associated with biometric access management tests

(f) Clearance Verification

- A – Revise clearance verification policy document
- A – Verify clearance verification policy is integrated into overall system and procedures
- A – Verify clearance verification procedures are enforced

(g) Need-to-Know Controls

- I – Direct need-to-know tests
- I – Enforce need-to-know policy
- A – Evaluate need-to-know requirements
- A – Evaluate results of need-to-know tests
- A – Implement need-to-know policy
- A – Prescribe need-to-know changes resulting from evaluation
- A – Prescribe oversight associated with need-to-know tests
- A – Revise need-to-know policy document
- A – Verify need-to-know policy is integrated into overall system and procedures
- A – Verify need-to-know procedures are enforced

(h) Password Management

- A – Prescribe oversight associated with password management tests
- A – Revise password management policy document
- A – Verify password management policy is integrated into overall system and procedures
- A – Verify password management procedures are enforced

(i) Roles and Responsibilities (RBAC – Role Based Access Control)

- A – Revise RBAC policy document
- A – Verify RBAC policy is integrated into overall system and procedures
- A – Verify RBAC procedures are enforced

(j) Unauthorized Access

- E – Discuss unauthorized access attempts
- A – Evaluate results of test of unauthorized access policy
- A – Perform test of unauthorized access procedures
- A – Prescribe changes resulting from evaluation
- A – Prescribe oversight for access policy
- A – Revise unauthorized access policy document
- A – Verify unauthorized access policy is integrated into overall system and procedures
- A – Verify unauthorized procedures are enforced

(2) Key Management**(a) COMSEC**

- E – List national COMSEC policies

- E – List national COMSEC procedures
- A – Revise policy document
- A – Verify COMSEC procedures are enforced

(b) Key Certificate Administration (EKMS)

- A – Revise policy document
- A – Verify EKMS management is integrated into overall system and procedures
- A – Verify EKMS procedures are enforced

(c) Key Escrow

- E – Explain national key escrow policies and procedures
- A – Revise policy document
- A – Verify key escrow procedures are enforced

(d) Peer-to-Peer Security

- A – Revise policy document
- A – Verify peer-to-peer security management is integrated into overall system and procedures
- A – Verify peer-to-peer security procedures are enforced

(e) Public Key Infrastructure (PKI)

- A – Verify PKI management is integrated into overall system and procedures
- A – Verify PKI procedures are enforced

(3) Configuration Management

- E – Identify configuration management requirements
- I – Direct configuration management tests
- I – Direct change control
- I – Enforce configuration management policy
- I – Enforce change control
- I – Explain configuration management
- I – Explain change control
- I – Explain configuration management requirements
- I – Perform security testing prior to implementation ensuring changes made to systems do not violate security policy
- I – Require accountability of copyrighted software in accordance with software licensing agreements
- A – Evaluate configuration management requirements
- A – Evaluate change control
- A – Evaluate results of configuration management tests
- A – Implement configuration management policy
- A – Implement change control
- A – Prescribe configuration management changes resulting from evaluation
- A – Prescribe oversight associated with configuration management tests

(4) Protective Technology

- E – Identify protective technology requirements
- I – Direct protective technology tests
- I – Enforce protective technology policy
- I – Explain protective technology requirements

- A – Evaluate protective technology requirements
- A – Evaluate results of protective technology tests
- A – Implement protective technology policy
- A – Prescribe oversight associated with protective technology tests
- A – Prescribe protective technology changes resulting from evaluation

(5) Media Security

- (a) FAX Security**
 - I – Enforce procedures governing FAX security
- (b) Lines (Fiber, Copper, Wireless)**
 - I – Enforce appropriate security measures for each type of media
 - I – Enforce security needs for leased lines
 - I – Enforce security needs for owned lines
- (c) Modems**
 - I – Enforce policy and practices for modem security
- (d) Phone Mail**
 - I – Enforce procedures governing phone mail security
- (e) TEMPEST**
 - I – Enforce procedures governing EMSEC/TEMPEST security
- (f) Voice Communication Security**
 - I – Enforce procedures governing voice communications security
- (g) Wireless communication security**
 - I – Enforce procedures governing wireless communications security

(6) Network Assurance

- (a) Network Security**
 - I – Direct network security tests
 - I – Enforce network security requirements
 - A – Evaluate results of network security tests
 - A – Monitor use of network security
 - A – Prescribe changes resulting from evaluation
 - A – Prescribe oversight associated with network security tests
- (b) Network Boundaries and Perimeters**
 - I – Direct network boundaries and perimeters security tests
 - I – Enforce network boundaries and perimeters security requirements
 - A – Evaluate results of network boundaries and perimeters security tests
 - A – Monitor use of network boundaries and perimeters security
 - A – Prescribe changes resulting from evaluation
 - A – Prescribe oversight associated with network boundaries and perimeters security tests

D. AUTOMATED SECURITY TOOLS

(1) Automated Security Tools

- E – Use expert system tools (i.e., audit reduction and intrusion detection) available
- I – Direct automated security tools tests
- I – Enforce use of automated security tools

- A – Evaluate results of automated security tools and tools tests
- A – Integrate use of automated security tools
- A – Monitor use of automated security tools
- A – Prescribe changes resulting from evaluation
- A – Prescribe oversight associated with use of automated security tools

(2) **Initiate Protective and/or Corrective Measures**

- I – Enforce protective or corrective measures
- I – Enforce security clearance, authorization, and need-to-know requirements

E. HANDLING MEDIA

(1) **Handling Media**

- I – Enforce media/information handling requirements

(2) **Labeling**

- I – Enforce security media/information marking requirements
- A – Verify labeling procedure policy is implemented

(3) **Marking of Media/Information Systems Oversight Office (ISOO) Rules**

- I – Enforce security media/information marking requirements
- A – Verify Information Systems Oversight Office (ISOO) procedure policy is implemented

(4) **Marking of Sensitive Information**

- I – Enforce security media/information marking requirements
- A – Verify marking procedure policy is implemented

(5) **Physical Controls & Accounting**

- I – Enforce security physical controls and accounting requirements
- A – Verify physical controls and accounting procedure policy is implemented

(6) **Remanence**

- E – Execute non-automated data remanence tools
- I – Enforce information remanence requirements
- A – Verify remanence procedure policy is implemented

(7) **Transportation**

- I – Enforce transportation security requirements
- A – Verify transportation procedure policy is implemented

(8) **Disposition of Classified Material**

- E – Explain disposition of classified media policies and procedures
- E – Define disposition reports
- A – Report discrepancies with disposition

F. INCIDENT RESPONSE

(1) **Criminal Prosecution**

- E – Discuss criminal prosecution requirements
- I – Enforce criminal prosecution requirements

(2) **Evidence Acceptability**

- I – Enforce rules on evidence acceptability
- A – Prescribe oversight associated with evidence acceptability in investigations

(3) **Evidence Collection and Preservation**

- I – Assist in evidence collection
- I – Discuss problems associated with evidence collection
- I – Enforce evidence collection and preservation security requirements
- A – Evaluate evidence collection procedures
- A – Monitor evidence collection and preservation security
- A – Prescribe changes resulting from evidence collection
- A – Verify that evidence collection and preservation policy is implemented

(4) **Legal and Liability Issues**

- E – Discuss legal liability issues
- E – Identify legal liability issues
- I – Discuss legal liability issues
- I – Enforce legal and liability security requirements
- I – Explain legal liability issues
- I – Summarize legal liability issues

4. REPORT ON SITE SECURITY STATUS

A. SECURITY CONTINUITY REPORTING

(1) Contingency Plans

- E – Define contingency plan reporting
- I – Report on status of restoration of information systems

(2) Continuity Plans

(a) **Reconstitution**

- E – Define continuity plan reporting
- E – Define reconstitution reporting
- A – Report implementation of Continuity plan
- A – Report status of reconstitution of systems

(b) **Restoration**

- E – Define restoration reports
- E – Define backup reports
- A – Report on status of back ups
- A – Report on status of restoration

(3) Disposition of Classified Material & Emergency Destruction Procedures (EDP)

- E – Define disposition reports
- E – Define EDP reports
- A – Report discrepancies with disposition
- A – Report implementation of EDP

(4) Monitoring and Auditing

(a) **Audit**

- I – Discuss auditing reports

(b) **Alarms, Signals, & Reports**

- E – Explain reporting audit alarms and signals
- A – Report audit alarms and signals

(c) **Assessments (e.g., surveys, inspections)**

- E – Explain how to report audit assessments
- A – Report findings and recommendations

(5) Identification & Authentication

(a) **Account Administration**

- E – Describe process to report unauthorized accounts
- A – Report unauthorized accounts

(b) **Password Management**

- E – Describe process to report insufficient passwords
- A – Report insufficient password

(c) **Unauthorized Access**

- I – Discuss what reporting is required for unauthorized access

A – Report unauthorized access

(6) Configuration Management

E – Describe configuration management reporting requirements

A – Report changes in configuration to SSM, viz., CIO, DAA, CTO, etc.

A – Report on recommendations for configuration management

A – Report security issues for configuration management

(7) Testing

E – Describe how various types of testing are reported

I – Prepare testing reports

A – Report adverse side effects of testing to SSM, viz., CIO, DAA, CTO, etc.

A – Report when testing is completed to SSM, viz., CIO, DAA, CTO, etc.

A – Report when testing is scheduled to SSM, viz., CIO, DAA, CTO, etc.

B. REPORT SECURITY INCIDENTS

(1) Computer Organizational/Agency Systems Emergency/Incident Response Team

E – Identify organizational/agency systems emergency/incident response team

E – Distribute organizational/agency systems emergency/incident response team reports and advisories

A – Report security issues to organizational/agency systems emergency/incident response team

A – Report violations, incidents, and breaches appropriately

(2) Security Incidents

A – Report security incidents in accordance with agency-specific/local policy to SSM, viz., CIO, DAA, CTO, etc. when information system compromised

A – Respond to attacks/incidents

(3) Security Violations Reporting Process (incident response)

E – Comply with agency specific/local directives when reporting to SSM, viz., CIO, DAA, CTO, etc.

E – Describe process of responding and reporting of security incidents

I – Assist users and managers with reporting

A – Report on evaluated damage done by an incident

A – Report recommended actions, changes, modifications to information assurance program and practices based upon an incident

A – Report results of an incident response

C. LAW

(1) Investigative Authorities

E – Identify agencies and offices responsible for investigating security incidents

I – Explain what information is reported to which agencies and offices

A – Report appropriate information as defined in security policy to appropriate agencies and offices

A – Report investigative efforts to SSM, viz., CIO, DAA, CTO, etc.

(2) Law Enforcement Interfaces (LEI)

- E – Describe how ISSO interfaces with law enforcement agencies
- E – Describe how to contact law enforcement interfaces (LEI)
- I – Explain how to use assistance from LEI
- A – Report and coordinate with LEI
- A – Report LEI activities to SSM, viz., CIO, DAA, CTO, etc.

(3) Witness Interviewing/Interrogation

- E – Assist appropriate authority in witness interviewing/interrogation
- E – Describe proper procedures to follow when conducting a witness interview
- E – Identify who can conduct interrogations (investigative agencies only)

(4) Entrapment

- I – Discuss notification requirements to use entrapment techniques
- A – Report use of entrapment techniques being instituted for compliance with policies and guidelines
- A – Verify that entrapment activities are approved by organizational/agency systems emergency/incident response team and SSM, viz., CIO, DAA, CTO, etc.
- A – Verify that entrapment in the legal sense does not occur

(5) Disgruntled Employees

- E – Identify notification requirements for handling disgruntled employees
- I – Know legal rights of disgruntled employees before reporting
- A – Report behavior of disgruntled employees to appropriate authorities
- A – Report identification of disgruntled employees to appropriate authorities

**D. REPORT SECURITY STATUS OF INFORMATION SYSTEM AS REQUIRED
BY SSM, VIZ., CIO, DAA, CTO, ETC.**

(1) Administrative Security Policies and Procedures

- E – Explain necessity of reporting on administrative security policies and practices
- I – Prepare report of non-compliance to SSM, viz., CIO, DAA, CTO, etc.
- I – Propose modifications to current policies and procedures
- A – Report recommendations for corrective/remedial action for non-compliance
- A – Report shortfalls in current policies and procedures

(2) Agency Specific Security Policies

- E – Describe how agency specific policies enhance overall security posture of information systems by defining operational environment
- I – Comply with agency specific security policies when reporting security status to SSM, viz., CIO, DAA, CTO, etc.

(3) Organizational/Agency Systems Emergency/Incident Response Team

- E – Explain how other sources of information can assist ISSO in providing additional information for reporting security status of information systems
- I – Compile information from various sources for compilation into status report
- A – Disseminate status report

(4) **Automated Systems Security Incident Support Team (ASSIST)**

- E – Explain how other sources of information can assist ISSO in providing additional information for reporting security status of information systems
- I – Compile information from various sources for compilation into status report
- A – Disseminate status report

(5) **Trade Journals, Bulletin Board System (BBS) Notices**

- E – Explain how other sources of information can assist ISSO in providing additional information for reporting security status of information systems
- I – Compile information from various sources for compilation into status report
- A – Disseminate status report

E. REPORT TO IG

Inspector General (IG) (External) Audit & Assessments

- E – Describe areas encompassed by report
- E – Identify appropriate reporting channels for IG
- A – Integrate IG results into report

5. SUPPORT CERTIFICATION AND ACCREDITATION

Ensure information system is accredited and certified if it processes sensitive information

A. CERTIFICATION FUNCTION

(1) Assessments (e.g., surveys, inspections)

- E – Prepare assessments for use during certification of information systems
- I – Develop assessments for purpose of certifying information systems
- I – Review assessments for purpose of certification of information systems

(2) Risk Assessment

- I – Direct risk assessment of information systems

(3) Technical Certification

- I – Direct technical certification of information systems

(4) Verification and Validation Process

- I – Direct verification and validation process as part of certification of information systems

B. ACCREDITATION FUNCTION

(1) ISSO

- E – Monitor system status post accreditation
- E – Initiate accreditation process
- I – Organize accreditation process
- I – Direct efforts of users in accreditation process
- A – Complete accreditation process
- A – Support obtaining SSM, viz., CIO, DAA, CTO, etc. approval

(2) Managers

- I – Ensure the re-accreditation of the system
- I – Direct efforts of Managers in accreditation process

(3) System Administrator (SA)

- E – Explain contents of Systems Security Plan (SSP)
- I – Direct efforts of SA in accreditation process
- I – Direct writing of SSP
- I – Write SSP for simple information system
- A – Write/maintain SSP
- A – Write SSP for complex information system

C. RESPOND TO SSM, VIZ., CIO, DAA, CTO, ETC. REQUESTS

(1) Approval to Operate

- E – Explain purpose and contents of Approval to Operate (ATO) to users
- I – Direct risk assessment to support granting an ATO
- A – Conduct risk assessment to support granting an ATO

A – Guide implementation of risk mitigation strategies necessary to obtain ATO

(2) Assessment Methodology

E – Explain C&A process for information system

I – Direct C&A effort for information systems

A – Conduct C&A effort for information systems

(3) Certification Statement

E – Explain purpose and contents of Certification Statement to users

I – Direct C&A effort leading to Certification Statement

A – Conduct C&A effort leading to Certification Statement

(4) Certification Tools

E – Discuss certification tools

E – Discuss ST&E plan and procedures

E – Recommend revisions to ST&E plan and procedures

E – Recommend use of specific certification tools

I – Direct use of certification tools

I – Review results of execution of certification tools

I – Review results of execution of ST&E plan and procedures

A – Analyze results of carrying out ST&E plan and procedures

A – Analyze results of certification tools

A – Develop security test and evaluation plan and procedure

A – Execute certification tools

(5) Identify Security Changes to SSM, viz., CIO, DAA, CTO, etc.

E – Differentiate security-related changes from non-security-related changes

E – Explain security-relevant changes to be made to information system

I – Determine if re-certification is warranted

(6) Interim Approval to Operate (IATO)

E – Explain purpose and contents of Interim Approval to Operate (IATO) to users

I – Direct risk assessment to support granting an IATO

A – Conduct risk assessment to support granting an IATO

A – Guide implementation of risk mitigation strategies necessary to obtain IATO

(7) Re-Certification

E – Explain purpose and process of re-certification

E – Identify information system that needs re-certification

I – Direct re-certification effort

A – Conduct re-certification effort

(8) Security Test & Evaluation (ST&E)

E – Discuss ST&E

A – Work with ST&E team to write test plan

(9) SSAA

E – Explain contents of SSAA

I – Direct writing of SSP

I – Recommend modifications to the SSAA

- I – Write SSAA for simple information system
- A – Influence certifier in development of SSAA to ensure mission
- A – Write SSAA for complex information system

(10) Type Accreditation

- E – Explain purpose and contents of type accreditation to users
- I – Direct risk assessment to support accreditation
- A – Conduct risk assessment to support accreditation
- A – Guide implementation of risk mitigation strategies necessary to obtain accreditation

(11) Waive Policy to Continue Operation

- E – Explain justification for waiver
- I – Conduct risk assessment to support granting waiver
- A – Guide implementation of risk mitigation strategies necessary to obtain waiver

ANNEX B

REFERENCES

The following references pertain to this instruction:

1. Common Criteria for Information Technology Security Evaluation, dated Aug 1999
2. DoD Directive 8000.1, Management of Information Resources and Information Technology, dated 27 Feb 2002
3. DoD Directive 8500.1, Information Assurance, dated 24 Oct 2002
4. DoD Instruction 8500.2, Information Assurance (IA) Implementation, dated 6 Feb 2003
5. DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), dated 30 Dec 1997
6. DoD 8510.1M, Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual, dated 31 Jul 2000
7. EO 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, dated 3 Apr 1984
8. EO 13231, Critical Infrastructure Protection in the Information Age, dated 16 Oct 2001 as amended by EO 13286, Transfer of Certain Functions to the Secretary of Homeland Security, dated 28 Feb 2003
9. Federal Information Processing Standards Publication (FIPS) Publication 31, Guidelines for Automatic Data Processing Physical Security and Risk Management, dated Jun 1974
10. Federal Information Processing Standards Publication (FIPS) Publication 65, Guideline for Automatic Data Processing Risk Analysis, dated 1 Aug 1993
11. Federal Information Processing Standards Publication (FIPS) 87, Guidelines for ADP Contingency Planning, dated 27 Mar 1981
12. Federal Information Processing Standards Publication (FIPS) Publication 102, Guideline for Computer Security Certification and Accreditation, dated 27 Sep 1983
13. National Computer Security Center (NCSC) TG-005, Trusted Network Interpretation (TNI), dated 31 Jul 1987
14. National Computer Security Center (NCSC)-TG-027, Version 1, A Guide To Understanding Information System Security Officer Responsibilities for Automated Information Systems, dated May 1992
15. National Computer Security Center (NCSC)-TG-029, Version 1, Introduction to Certification and Accreditation, dated Jan 1994
16. NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, dated Oct 1995
17. NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, dated Sep 1996
18. NIST SP 800-16, Information Technology Security Training Requirements: A Role and Performance-based Model, dated Apr 1998
19. NIST SP 800-18, Guide for Development of Security Plans for Information Technology Systems, dated Dec 1998

20. NIST SP 800-64, Security Considerations in the Information Systems Development Life Cycle, dated Oct 2003
21. NSD 42, National Policy for the Security of National Security Telecommunications and Information Systems, dated 5 Jul 1990
22. NSTISSD 501, National Training Program for Information Systems Security (INFOSEC) Professionals, dated 16 Nov 1992
23. NSTISSI No.1000, National Information Assurance Certification and Accreditation Process (NIACAP), dated Apr 2000
24. CNSSI No. 4009, National Information Assurance (IA) Glossary, dated May 2003
25. NSTISSP No. 11, Revised Fact Sheet, National Assurance Information Acquisition Policy, dated July 2003
26. OMB Circular No. A-130, Revised (Transmittal Memorandum No. 4), Management of Federal Information Resources, dated 30 Nov 2000
27. OMB Memorandum M-00-07, Incorporating and Funding Security in Information Systems Investments, dated 28 Feb 2000
28. OMB Memorandum M-01-08, Guidance on Implementing the Government Information Security Reform Act, dated 16 Jan 2001
29. OMB Memorandum M-01-24, Reporting Instructions for the Government Information Security Reform Act, dated 22 Jun 2001
30. OMB Memorandum M-02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones, dated 17 Oct 2001
31. Code of Federal Regulations, 5 C.F.R. §903 *et seq.*, Employees Responsible for the Management or Use of Federal Computer Systems
32. PL 93-579, 5 U.S.C. §552a, the Privacy Act of 1974
33. PL 107-347, E-Government Act of 2002, Title III, Federal Information Security Management Act (FISMA), 17 Dec 2002
34. PL 104-106, Division E, the Information Technology Management Reform Act (Clinger-Cohen Act) of 1996
35. PL 106-398, Title X, Subtitle G, the Government Information Security Reform Act (GISRA), dated 30 Oct 2002
36. The President's National Strategy to Secure Cyberspace, dated Feb 2003

F. CNSS Standard NTSTISSI 4015

a. Course Mapping Details

Welcome Barbara Ciaramitaro, it is Monday, August 16, 2010 at 03:37:59 PM
You are currently viewing a report for NSTISSI 4015 sorted by element.

▼ **10. MAINTENANCE OF THE SSAA**

▼ **a. Life-Cycle Security Planning**

▼ **1) discuss, when consulted, proposed changes to the SSAA**

▼ *NO SUB-CATEGORY

[HSCJ 202](#)
[MISM 661](#)

▼ **2) propose, where required, a need for recertification and reaccreditation**

▼ NO SUB-CATEGORY

[HSCJ 202](#)
[MISM 661](#)

▼ **3) interpret, when consulted, changes that may affect the existing certification**

▼ NO SUB-CATEGORY

[HSCJ 202](#)
[MISM 661](#)

▼ **b. Documentation Policies**

▼ **1) appraise the documentation policies for continued applicability**

▼ *NO SUB-CATEGORY

[HSCJ 202](#)
[MISM 661](#)

▼ **2) identify the documentation policies for updates**

▼ NO SUB-CATEGORY

[HSCJ 202](#)
[MISM 661](#)

▼ **3) verify changes against the original documentation policies**

▼ NO SUB-CATEGORY

[HSCJ 202](#)
[MISM 661](#)

▼ **c. Configuration Control/Change Management**

▼ **1) appraise the configuration control for continued applicability**

▼ *NO SUB-CATEGORY

[HSCJ 202](#)
[MISM 661](#)

▼ **2) identify the configuration control in place versus that which has been specified in the current SSAA**

▼ NO SUB-CATEGORY

[HSCJ 202](#)
[MISM 661](#)

▼ **3) list proposed changes to the previously approved system configuration and/or operating environment, to include system retirement**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **4) analyze the above changes to determine if an assessment of the impact is required**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **5) outline the process for an assessment of the impact of changes to the existing SSAA**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **6) revise the SSAA in accordance with the configuration changes**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **d. Maintenance of Configuration Documents**

- ▼ **1) appraise the maintenance of configuration documents**

- ▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **2) compare the maintenance of configuration documents for conformance to the SSAA**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **e. Periodic Review of System Life-cycle**

- ▼ **1) appraise the periodic review of the system/product life-cycle for conformance to the SSAA**

- ▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **2) initiate the periodic review of the system/product life-cycle for conformance to the SSAA**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **3) report on the periodic review of the system/product life-cycle**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **f. Communicate Results**

- ▼ **1) report the results of changes to the SSAA to the accreditor (DAA).**

- ▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **g. Convey Magnitude of Risk**

▼ **1) identify the inherent and residual risks and the potential corrective approaches to the accreditor (DAA).**

▼ *NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **h. Brief and Defend ST&E Results**

▼ **1) prepare and deliver the ST&E results to the accreditor (DAA).**

▼ *NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **1. DOCUMENTING MISSION NEED**

▼ **a. Knowledge and/or Awareness of Security Laws**

▼ **1) identify relevant nation-state security laws, treaties, and/or agreements**

▼ *NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **2) interpret nation-state security laws, treaties, and/or agreements in relation to mission accomplishment**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **3) relate the identified nation-state security laws, treaties, and/or agreements to the mission needs**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **4) discuss identified nation-state security laws, treaties, and/or agreements with involved site personnel**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **5) explain interpretation in support or denial of certification to involved site personnel**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **b. Coordination with Related Disciplines**

▼ **1) identify the related disciplines required for accomplishing the IS certification**

▼ *NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **2) discuss mission-specific discipline relationships and IS requirements with involved site personnel**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **c. Understand Mission**

▼ **1) study the mission critical elements, to include system mission, functions, and system interfaces**

▼ *NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **2) verify that mission critical elements are completely identified (e.g., operational procedures and classification requirements)**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **3) confirm the mission description is complete as it relates to documented IS needs, to include system life cycle**

▼ NO SUB-CATEGORY

HSCJ 202
ISYS 411
MISM 661

▼ **4) discuss the interpretation of mission critical elements in support or denial of certification with involved site personnel**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **5) research and discuss mission operational environment (e.g., charter, scope of authorities, activation call-up procedures, Information Warfare Condition (INFOCON) processes)**

▼ NO SUB-CATEGORY

HSCJ 202
ISIN 330
MISM 661

▼ **d. Contingency Planning**

▼ **1) assess the need for contingency planning**

▼ *NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **2) study the identified critical contingency elements**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **3) confirm that the critical elements of mission contingency planning have been identified in relation to the specific operational environment**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **4) discuss the critical contingency elements and IS requirements in relation to mission accomplishment to assure system recovery and reconstitution**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **5) explain the appraisal in support or denial of certification to involved site personnel**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **6) verify that the documented mission need elements are identified in the critical system contingency plan**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **2. CONDUCTING REGISTRATION**

▼ **a. System Certification Memorandum of Understanding (MOU) or Other Instruments**

▼ **10) verify the integrity of an MOU or other instruments**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **11) report the status of MOUs or other instruments to the DAA**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **1) propose the development of an MOU or other appropriate instruments**

▼ *NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **2) describe the purpose, scope, and contents of a particular MOU or other instruments**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **3) identify the respective parties and their roles**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **4) discuss anticipated challenges to an MOU or other instruments**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **5) explain the various details of an MOU or other instruments**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **6) interpret the agreements specified in an MOU or other instruments**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

- ▼ **7) use an MOU or other instruments to define the responsibilities and requirements for team members with specialized knowledge**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **8) use an MOU or other instruments to assist in SSAA and other policy development**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **9) comply with the requirements of a system certification MOU or other instruments**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **b. Collect Security Requirements**
 - ▼ **1) describe the security requirement collection process**
 - ▼ *NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
 - ▼ **2) research security requirements**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
 - ▼ **3) describe to the DAA, program management office (PMO), etc., the appropriate requirements for system security**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **c. Knowledge and/or Awareness of Security Laws Required for System Being Evaluated**
 - ▼ **1) explain the applicable laws, statutes, and regulations**
 - ▼ *NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
 - ▼ **2) discuss how the system will operate according to legal mandates**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
 - ▼ **3) identify the organizational point of contact for legal advice**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **d. Audit Collection Requirements**
 - ▼ **1) describe the audit collection requirements relative to system certification**
 - ▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 2) assist in the identification of audit requirements

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ e. Coordination with Related Disciplines

▼ 1) discuss the role of related security disciplines in the overall protection of the system

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 2) describe the related security disciplines and how they apply to the certification of the system

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 3) identify the related disciplines needed for the certification team

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ f. Configuration Control Policies

▼ 1) advise in the development of configuration control policies

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 2) assess the system configuration control plan against policy

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 3) report to the DAA the deficiencies/discrepancies in the configuration control policy

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ g. Contingency Planning

▼ 1) assess the need for contingency planning

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 2) propose contingency planning activities

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 3) discuss the contingency planning process

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 4) **assess contingency planning**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 5) **report to the DAA any discrepancies or deficiencies in contingency plans**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **h. Personnel Selection**

▼ 1) **explain the criteria for personnel selection for the certification team**

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 2) **perform personnel selection for the certification team based on the requisite skills for the IS involved**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **i. Roles and Responsibilities**

▼ 1) **identify and define the roles and responsibilities of the certification team**

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 2) **propose the roles and responsibilities of individual certification team members**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **j. Scope and Parameters of the Certification**

▼ 1) **describe, define, and present the scope and parameters of the certification.**

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **k. Set Certification Process Boundaries**

▼ 1) **define and describe the certification process boundaries**

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 2) **identify and propose the boundaries of the certification process**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **l. Risk Management**

▼ 1) **select the appropriate risk management methodology for the IS to be certified**

▼*NO SUB-CATEGORY

HSCJ 202

MISM 661

▼2) discuss the risk management methodology and threat mitigation using examples and explanations

▼NO SUB-CATEGORY

HSCJ 202

MISM 661

▼3) describe the risk management methodology appropriate to the certification of the system

▼NO SUB-CATEGORY

HSCJ 202

MISM 661

▼m. System Description

▼1) verify that the system description is consistent with the documented mission need.

▼*NO SUB-CATEGORY

HSCJ 202

MISM 661

▼n. System Security Policy

▼1) ensure the development and inclusion of a comprehensive system security policy

▼*NO SUB-CATEGORY

HSCJ 202

MISM 661

▼2) assess policy to ensure it conforms with applicable laws and directives and data owner requirements

▼NO SUB-CATEGORY

HSCJ 202

MISM 661

▼o. Budget/Resources Allocation

▼1) define and describe budget elements related to the certification process

▼*NO SUB-CATEGORY

HSCJ 202

ISYS 411

MMBA 640

MISM 661

▼2) identify the resource requirements necessary to accomplish the certification process

▼NO SUB-CATEGORY

HSCJ 202

ISYS 411

MMBA 640

MISM 661

▼p. Timeline/Scheduling

▼1) establish certification milestones

▼*NO SUB-CATEGORY

HSCJ 202
ISYS 411
MMBA 640
MISM 661

▼ 2) relate the milestones to roles and responsibilities

▼ NO SUB-CATEGORY

HSCJ 202
ISYS 411
MMBA 640
MISM 661

▼ q. Life-Cycle System Security Planning

▼ 1) assess life-cycle security planning against requirements, directives and laws

▼ *NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ 2) describe life-cycle security planning

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ 3) assist in life-cycle security planning with respect to the certification requirements

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ 3. PERFORMING NEGOTIATION

▼ a. Life-Cycle System Security Planning

▼ 1) explain life-cycle system security planning

▼ *NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ 2) propose life-cycle system security attributes to involved site personnel

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ 3) propose improvements to the plans developed by site personnel

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ b. Set Certification Process Boundaries

▼ 1) discuss setting certification boundaries

▼ *NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ 2) describe setting certification boundaries

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **3) influence certification boundaries**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **4) justify setting certification boundaries**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **5) report the setting of certification boundaries as part of the SSAA**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **c. Risk Management**

▼ **1) appraise elements of life-cycle activity versus the risk management process components of mission, vulnerabilities, threat, and countermeasures to determine if system development activity is ready for c**

▼ *NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **d. Knowledge and/or Awareness of Security Laws**

▼ **1) use the knowledge and awareness of security laws to ensure system development activities follow legal guidelines**

▼ *NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **4. PREPARING SSAA**

▼ **a. Access Control Policies**

▼ **1) categorize access control policies**

▼ *NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **2) describe access control policies**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **3) relate access control policies to appropriate "umbrella" guidance and policies**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **b. Security Policies and Procedures**

▼ **1) define and understand the topics that security policies and procedures must address as part of the certification process**

▼ *NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **2) discuss the impact of policy and procedures on risk and operations**

- ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **3) explain how the system operating policies and procedures define the implementation of the security requirements**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **4) integrate the identified security policies and procedures (i.e., audit policies, access control policies) as minimum requirements into the ST&E plan**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **5) interpret the relationship between security policy and procedures and the security requirements**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **6) assist the DAA, program manager (PM), and user in understanding the security policies and procedures**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **7) describe the security solutions and implementations that meet the specified system security requirements**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **c. Documentation Policies**
 - ▼ **1) identify documentation policies that apply to the preparation of the SSAA**
 - ▼ *NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
 - ▼ **2) ensure that the appropriate documentation policies are followed in preparing the SSAA**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **d. Requirements Derivation**
 - ▼ **10) explain the security requirements in order to develop a common understanding among the DAA, PM, and Certification Authority**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
 - ▼ **1) categorize security certification requirements**
 - ▼ *NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661

- ▼ **2) discuss how technical and non-technical security requirements are derived**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **3) identify requirements that are applicable to the system under certification and accreditation**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **4) identify the source of the security requirements**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **5) identify the source of the security requirements for use during negotiations, development of the SSAA, and compliance validation**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **6) interpret security requirements for the specific mission, environment, data classification level, and architecture**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **7) summarize the security requirements and construct a requirements traceability matrix (RTM)**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **8) use security requirements to assist in the development of ST&E plans**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **9) verify that security certification requirements are included in the ST&E plan**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **e. Understand Mission**
 - ▼ **1) describe the system mission focusing on the security relevant features of the system required for the SSAA**
 - ▼ *NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
 - ▼ **2) discuss the purpose of the system and its capabilities in the SSAA**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
 - ▼ **3) explain the impact of the mission statement on security requirements**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 4) summarize the mission and prepare a summary for the SSAA

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 5) use the mission statement to identify applicable security certification requirements in the SSAA

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ f. Security Domains

▼ 1) identify any specific security domains as they apply to the system mission and function

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 2) relate the interactions between different security domains in support of the system mission and functions

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ g. System Description

▼ 10) identify the system acquisition strategy and system life-cycle phase

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 11) use the data sensitivity and labeling requirements to determine the system classification

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 1) appraise the system concept of operations (CONOPS)

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 2) assess the system's criticality and its impact on the level of risk that is acceptable

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 3) define the system user's characteristics and clearances

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 4) define the security clearances of the user population and the access rights to restricted information

- ▼ NO SUB-CATEGORY
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **5) define the type of data and data sensitivity**
 - ▼ NO SUB-CATEGORY
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **6) describe the system CONOPS and security CONOPS in the SSAA**
 - ▼ NO SUB-CATEGORY
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **7) describe the system criticality in the SSAA**
 - ▼ NO SUB-CATEGORY
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **8) describe the system functions and capabilities**
 - ▼ NO SUB-CATEGORY
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **9) examine the mission to determine the national security classification of the data processed**
 - ▼ NO SUB-CATEGORY
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **h. Environment and Threat Description**
 - ▼ **1) derive the system operating environment and threat descriptions from the mission documentation**
 - ▼ *NO SUB-CATEGORY
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼ **2) prepare a description of potential threats based upon an analysis of the operating environment, and the system development environment for inclusion in the certification reports for the DAA**
 - ▼ NO SUB-CATEGORY
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **i. System Operating Environment**
 - ▼ **1) describe the administrative security procedures appropriate for the system being certified**
 - ▼ *NO SUB-CATEGORY
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼ **2) analyze the physical environment in which the system will operate; address all relevant parts of the system's environment, including descriptions of the physical, administrative, developmental, and**
 - ▼ NO SUB-CATEGORY
 - [HSCJ 202](#)
 - [MISM 661](#)

▼ **3) describe the security features that will be necessary to support site operations (the physical security description should consider safety procedures for personnel operating the equipment)**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **4) identify maintenance procedures needed to ensure physical security protection against unauthorized access to protected information or system resources**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **5) identify procedures needed to counter potential threats that may come from inside or outside of the organization**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **6) identify the physical support features of the facility, including air conditioning, power, sprinkler system, fences, and extension of walls from true-floor to true-ceiling construction, sensitive s**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **7) determine if training procedures match the users' levels of responsibility, and provide information on potential threats and how to protect information**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **8) identify aspects of physical security, such as a defined secure work area; the means used to protect storage media (e.g., hard drives and removable disks); protecting access to workstation ports (e**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **j. System Development, Integration, and Maintenance Environment**

▼ **1) describe the system development approach and the environment within which the system will be developed and maintained**

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **2) describe the information access and configuration control issues for the system**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **3) determine the appropriate types of system development and maintenance environments**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **k. Threat Description and Risk Assessment**

- ▼ 1) define, in conjunction with the system owner, the potential threats that can affect the confidentiality, integrity, and availability of the system; clearly stating the nature of the threa

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ 2) identify threats, such as penetration attempts by hackers, damage or misuse by disgruntled or dishonest employees, and misuse by careless or inadequately trained employees

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ 3) identify unintentional human error, system design weaknesses, and intentional actions on the part of authorized, as well as unauthorized users that can cause these events

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ 4) describe insider threat, including the good intentions of a trusted employee who circumvents security in order to accomplish the job

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **i. System Architectural Description**

- ▼ 10) identify and include diagrams or text that clearly delineate the components that are to be evaluated as part of the C&A task

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ 11) identify components which are not to be included in the evaluation

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ 12) prepare a high level overview of the types of hardware, software, firmware, and associated interfaces envisioned for the completed system

▼ NO SUB-CATEGORY

HSCJ 202

ISYS 325

MISM 670

MISM 661

- ▼ 1) describe the accreditation boundary of the system

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **2) describe the system architecture including the configuration of any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, manage**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **3) describe the system's internal interfaces and data flows**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **4) identify and describe the system's external interfaces and the relationship between the interfaces and the system**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **5) describe the proposed and appropriate hardware and its function (NOTE: hardware is the physical equipment, as opposed to programs, procedures, rules, and associated documentation);**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **6) describe the proposed and appropriate software and its intended use (NOTE: software includes the entire set of application programs, software procedures, software routines, and operating system)**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **7) determine the types of data and the general methods for data transmission (NOTE: if specific transmission media or interfaces to other systems are necessary, these needs may influence the security)**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 670
 - MISM 661
- ▼ **8) develop an overview of the internal system structure including the anticipated hardware configuration, application software, software routines, operating systems, remote devices, communications**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **9) develop diagrams or text to explain the flow of critical information from one component to another**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **m. Identify C&A Organizations and Resources**
 - ▼ **1) enlist the assistance of a contractor team or other government organizations (NOTE: the CA has the responsibility to form the team, coordinate the C&A activities, conduct the analysis,**

- ▼ *NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ 2) identify the appropriate statutory authorities, and the resource and training requirements necessary to conduct the certification
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ 3) identify the organizations, individuals, and titles of the key authorities involved in the C&A process
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ 4) determine the certification team's roles and responsibilities
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ 5) form the C&A team after the CA knows the certification level and tasks required
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ 6) identify the roles of the certification team members as needed and their responsibilities
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ 7) include team members who have composite expertise in the whole span of activities required, and who are independent of the system developer or PM
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ n. Tailor the Agency-specific C&A Guidelines (e.g., NIACAP, DITSCAP) and Prepare the C&A Plan
 - ▼ 10) determine the appropriate certification analysis level and adjust the C&A guideline activities to the program strategy and system life
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
 - ▼ 11) determine where to focus the analysis and testing
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
 - ▼ 12) identify the appropriate level of effort
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - ISYS 411
 - MMBA 640

MISM 661

- ▼ **1) adjust and document the C&A guideline (e.g., NIACAP, DITSCAP) activities to fit the program strategy**

- ▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **2) conduct a review of the C&A guideline plan and SSAA by the DAA, CA, PM, and user representative**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **3) determine the skills needed to perform the analysis and the supporting documentation**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **4) prepare a process diagram of the system life-cycle activities and identify the current phase of life-cycle activity;**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **5) schedule the C&A guideline activities to meet the system schedule (for example, if the system has already completed preliminary design,**

- ▼ NO SUB-CATEGORY

HSCJ 202

ISYS 411

MMBA 640

MISM 661

- ▼ **6) tailor the C&A process as agreed upon in the SSAA**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **7) tailor the C&A guideline process to the system life-cycle at the current system phase or activity**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **8) tailor the process to the incremental development strategy (if one is used)**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **9) tailor the security activities to system development activities to ensure that the security activities are relevant to the process and**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **o. Prepare SSAA Added Material**

- ▼ **1) consolidate documentation, drawing together all pertinent materials into a logical, sequential, and coherent document which will support the DAA's decision to approve or disapprove**

- ▼ *NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ **2) identify constraints, assumptions, and dependencies of the C&A process being implemented**

- ▼ NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ **3) identify the conditions under which certification activities were accomplished**

- ▼ NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ **p. Requirements Traceability**

- ▼ **1) develop the security certification test plan documentation**

- ▼ *NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ **2) develop the ST&E evaluation report documentation**

- ▼ NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ **3) identify the source of the security requirements for use during negotiations, development of the SSAA, and compliance validation**

- ▼ NO SUB-CATEGORY

- HSCJ 202

- ISYS 411

- MISM 661

- ▼ **4) specify the required security evaluation documentation**

- ▼ NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ **5) use security requirements to develop the ST&E plans and procedures**

- ▼ NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ **6) develop security certification test procedures**

- ▼ NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ **7) outline any unique certification analysis documentation requirements**

- ▼ NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ **5. SUPPORTING SYSTEMS DEVELOPMENT**

▼ **a. Coordination with Related Disciplines**

▼ 1) explain to the development team and to the accreditor the need for coordination with related disciplines

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 2) perform coordination with the various offices responsible for the related disciplines

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 3) verify coordination with related security disciplines, e.g., physical, emanations, personnel, operations, and cryptographic security

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **b. Configuration Control**

▼ 1) appraise current system configuration control

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 2) discuss configuration control with the development team for compliance with required INFOSEC policy and technology;

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 3) propose configuration control changes

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 4) report the configuration control deficiencies to the developer

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 5) verify that the activities associated with configuration control, i.e., physical and functional audits, inventory of the hardware and software components, etc., are adequately documented a

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **c. Information Security Policy**

▼ 1) identify applicable information security policy

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 2) explain information security policy to the development team for the secure operation of the system

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ 3) use information security policy to ensure the appropriate secure operation of the system

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **d. Life-Cycle System Security Planning**

- ▼ 1) appraise the life-cycle system security planning proposed by the development team

- ▼ *NO SUB-CATEGORY

HSCJ 202

ISYS 411

MMBA 640

MISM 661

- ▼ 2) assist with the information security planning for life-cycle system security

- ▼ NO SUB-CATEGORY

HSCJ 202

ISYS 411

MMBA 640

MISM 661

- ▼ 3) explain the life-cycle system security planning to the development team

- ▼ NO SUB-CATEGORY

HSCJ 202

ISYS 411

MMBA 640

MISM 661

- ▼ 4) influence the development team's approach to life-cycle system security planning

- ▼ NO SUB-CATEGORY

ISYS 411

MMBA 640

MISM 661

- ▼ 5) verify that life-cycle system security planning has been accomplished

- ▼ NO SUB-CATEGORY

HSCJ 202

ISYS 411

MMBA 640

MISM 661

- ▼ **e. Parameters of the Certification**

- ▼ 1) propose alterations to the parameters of the certification process as the system development progresses and the design is modified

- ▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ 2) compare the parameters of the certification to those of similar systems or during parallel certification

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **3) determine the parameters of the certification to ensure mission accomplishment**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **4) explain the parameters of the certification to system developers and maintainers**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **5) use the parameters of the certification**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **6) verify adherence to the parameters of the certification**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **f. Principles and Practices of Information Security**

▼ **1) understand the principles and practices of information security**

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **2) identify principles and practices of information security that pertain to the certification**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **3) adhere to recognized principles and practices of information security**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **4) explain the principles and practices of information security that pertain to the certification to the developers**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **g. Network Vulnerabilities**

▼ **1) identify any network vulnerabilities for the system developers and maintainers**

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 662

▼ **2) demonstrate to the system developers and maintainers the network vulnerabilities that are present during the development of the system**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

MISM 662

▼ **3) evaluate the impact of network vulnerabilities**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

MISM 662

▼ **4) explain unacceptable network vulnerabilities to the developers**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

MISM 662

▼ **5) respond to network vulnerabilities by suggesting corrective measures when possible**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

MISM 662

▼ **6) stay current on network vulnerabilities**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

MISM 662

▼ **h. Security Engineering**

▼ **1) assist developers and maintainers with system security engineering principles as required for information security and certification and accreditation**

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **2) define security engineering principles that are applicable to information security**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **3) explain security engineering principles and practices**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **4) review security engineering principles and practices for compliance with information security policies**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **5) outline best security engineering practices as defined by the National Information Assurance Partnership (NIAP)**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **i. Access Control Policies**

▼ **1) be aware of access control policies;**

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **2) evaluate for the developers and maintainers the strengths and weaknesses of access control policies**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **3) explain the need for access control policies**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **4) identify to the developers and maintainers access control policies that are applicable to information security**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **5) recommend access control policy changes that are appropriate for the system being certified**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **6. PERFORMING CERTIFICATION ANALYSIS**

▼ **a. Access Control**

▼ **10) appraise whether the identification and authentication mechanism can correctly identify users and/or processes;**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **11) identify the requirement for discretionary/mandatory access controls (DAC/MAC)**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **12) explain to other team members and managers how access privileges are set**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **13) match data ownership and responsibilities with access control rights**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **14) match the requirements for respective access control features with appraised controls implemented**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **15) match the access control requirements with user roles and group management**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **16) determine the security countermeasures to implement effective access control**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **17) verify the contents of the user registry and access control tables**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **18) verify the effectiveness of password management software in enforcing policies and procedures**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **19) identify representative processes which must use an appropriate identification and authentication mechanism**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **1) appraise access control privilege assignment**
 - ▼ *NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **20) propose the security test and evaluation plan/procedures and schedule to test and evaluate agreed upon security countermeasures for access control**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **21) report recommended changes to the implemented access control mechanisms as needed to meet the requirements identified in the access control policies**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **2) appraise access controls defined as appropriate for the IS under review for subjects (e.g., local and remote users and/or processes)**
 - ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **3) appraise access controls for objects (e.g., data, information, and applications)**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **4) appraise access controls for privileged users and/or processes**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **5) appraise management of the access control tables and lists**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **6) appraise identification and authentication mechanisms which identify users and/or processes**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **7) appraise the implementation of user privileges and group management assignments**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **8) appraise managed and default file permission settings and factory settings**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **9) appraise the effectiveness of password management implemented to enforce policies and procedures**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **b. Audits**

▼ **10) appraise the use of audit information to validate the proper operation of automated system security capabilities**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **11) identify the audit elements and capabilities available on the system being evaluated**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **12) identify the audit event characteristics and their granularity (i.e., type of event, success/failure, date/time stamp, user ID)**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **13) summarize the data which supports trend analysis**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **14) verify that the audit elements capture information that meets specified security requirements**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **15) verify that the audit log overflow policy is correctly implemented**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **16) verify that audit procedures exist to implement the policy (i.e., data reviews, audit retention and protection, response to alerts, etc)**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **17) verify that audit processes support interpretation of the audit data**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **18) verify that the audit retention capability meets the system security requirements**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **19) verify that protections are in place to prevent the audit trails from being modified by any means, including direct edits of media or memory**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **1) appraise the system's ability to produce viable, inclusive audit data for review and analysis (e.g., selection capabilities for review of audit information);**

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **20) report the audit collection requirements to meet a stated authorization policy**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **21) report any alternative means to satisfy the audit collection requirements**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **22) propose aperiodic security test and evaluation plans and procedures to test and evaluate agreed upon audit functionality and events**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **23) verify that system resources are sufficient to log all required events**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **24) interpret the audit policy to be implemented (to include which events are to be recorded, what action should occur when the log fills, how long audits are to be retained, etc.)**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **25) determine the impact of audit requirements on the system operation requirements**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **26) appraise the capabilities of the add-on audit analysis and intrusion detection tools that are implemented**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **2) appraise the alert capabilities provided by audit/intrusion detection tools**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **3) verify the criteria for generating alerts provided by audit/intrusion detection tools**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **4) appraise the availability of audits including recovery from permanent storage**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **5) appraise the identification of anomalies which indicate successful violation/bypass of security capabilities**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **6) appraise the inherent audit capabilities and the proposed implementation**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **7) appraise the processes for analyzing audit information**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **8) appraise the report generation capability**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **9) appraise the use of audit information to identify attempts to violate/bypass the proper operation of system security capabilities**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **c. Applications Security**

▼ **1) appraise the effectiveness of applications security mechanisms and their interactions with other systems and network security mechanisms**

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **2) differentiate between the operating system and application system security features**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **3) propose security test and evaluation plans and procedures to test and evaluate agreed upon security countermeasures provided by application security mechanisms**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **d. Confidentiality, Integrity and Availability (CIA)**

▼ **1) explain the stated system requirements for confidentiality, integrity, and availability in the system design/SSAA documentation**

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **2) appraise the network architecture and what security mechanisms are used to enforce the CIA security policy**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **3) appraise the network security posture in light of the CONOPS and the abilities of the expected users and system administrators**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **e. Countermeasures**

- ▼ **1) appraise the requirements for additional countermeasures based on the security policy being implemented (e.g., routers, firewalls, guards, intrusion detection devices)**

- ▼ *NO SUB-CATEGORY

- HSCJ 202
 - MISM 670
 - MISM 661

- ▼ **2) study the security countermeasures documented in the SSAA**

- ▼ NO SUB-CATEGORY

- HSCJ 202
 - MISM 670
 - MISM 661

- ▼ **3) propose security test and evaluation plans and procedures to test and evaluate agreed upon security countermeasures documented in the SSAA**

- ▼ NO SUB-CATEGORY

- HSCJ 202
 - MISM 670
 - MISM 661

▼ **f. Documentation**

- ▼ **1) identify the documentation of security-related function parameters, defaults and settings**

- ▼ *NO SUB-CATEGORY

- HSCJ 202
 - MISM 661

- ▼ **2) report the review of the documentation, noting the adequacy of detail**

- ▼ NO SUB-CATEGORY

- HSCJ 202
 - MISM 661

- ▼ **3) identify the deficiencies in the system documentation, whether they be missing documents or inadequate detail in the existing documentation**

- ▼ NO SUB-CATEGORY

- HSCJ 202
 - MISM 661

▼ **g. Network Security**

- ▼ **1) appraise the network connectivity policy and the proposed implementation for connection**

- ▼ *NO SUB-CATEGORY

- HSCJ 202
 - MISM 670
 - MISM 661

- ▼ **2) appraise the security requirements for interconnectivity with other systems/networks**

- ▼ NO SUB-CATEGORY

- HSCJ 202
 - MISM 670
 - MISM 661

▼ **3) verify that formal approvals have been granted for other systems and networks for which interconnectivity is sought**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 670

MISM 661

▼ **4) appraise the security attributes of both the data and users accessing the connected system to determine whether additional security requirements result**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 670

MISM 661

▼ **5) propose security test and evaluation plans and procedures to test and evaluate agreed upon security countermeasures for network connectivity**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 670

MISM 661

▼ **h. Maintenance Procedures**

▼ **1) appraise the proposed system maintenance and upgrade procedures to ensure that they comply with configuration management procedures (e.g., remote software updates).**

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **i. Operating System Security**

▼ **1) appraise the documentation and system configuration of security function defaults and settings, ensuring that all inappropriate factory defaults have been changed**

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **2) appraise how the system handles error conditions**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **3) appraise the system recovery capability during loss of power situations**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **4) assess and report any variance between documented and actually installed software and operating systems**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **5) propose security test and evaluation plan/procedures to test and evaluate agreed upon security countermeasures enforced by the operating system**

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 6) verify that capabilities are employed to enforce the protection of the operating system by preventing programs or users from writing over system areas

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 7) verify that protections are in place to prevent configuration files and pointers that can run in a supervisory state from unauthorized access or unauthorized modifications, deletion

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 8) verify that protections are in place to prevent the operating system kernel from being modified by any process, program or individual except through an approved organizational confi

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ j. Vulnerabilities

▼ 1) identify vulnerabilities inherent to the system's specific operating system, applications, and network configuration

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

MISM 662

▼ k. Contingency Operations

▼ 1) appraise whether the disaster recovery mechanism adequately addressees the needs of the site

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 2) appraise whether the plan sufficiently protects the security of the information and the investment made in life-cycle security processes

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 3) match the requirements for disaster recovery/continuity of operation with mission requirements

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 4) match the requirements for emergency destruction procedures with mission requirements

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **7. CERTIFICATION EVALUATION**

▼ **a. Evaluation Techniques**

- ▼ 1) use appropriate evaluation techniques, e.g., documentation review, automated tools, and written test plan and procedures, etc., in the conduct of the security test and evaluation

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ 2) choose the evaluation technique(s) to exercise and evaluate security countermeasures or capabilities documented in the SSAA

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ 3) generate and/or validate the security test and evaluation plan and procedures

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **b. Access Control**

- ▼ 1) verify that access controls meet the criteria established in the SSAA

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ 2) document the results of the ST&E access control tests

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ 3) describe the ST&E testing results for access controls

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **c. Contingency Planning/Testing**

- ▼ 1) appraise the effectiveness of the contingency plan as described in the SSAA

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ 2) document the effectiveness of the contingency plan

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ **d. Audit Trail**

- ▼ 1) demonstrate that the audit trail is secure from unauthorized alteration and deletion

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 2) document the results

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 3) appraise whether the audit trail meets the requirements as defined in the SSAA and document the results

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ e. Intrusion Detection

▼ 1) verify the presence of intrusion detection capabilities as defined in the SSAA and document the results

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 2) demonstrate that the intrusion detection mechanisms work as outlined in the SSAA and document the results

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 3) analyze the effectiveness of the intrusion detection capabilities and document the results

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ f. Security Processing Mode

▼ 1) verify that the security processing mode has been identified

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 2) justify any suggested change in the security processing mode, if found to be inadequate or inappropriate, and document the results

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ 3) appraise whether or not the defined security processing mode is adequate for approving system certification, and document the results

▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

▼ g. Automated Security Tools

▼ 1) identify appropriate security tools and document the results

▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **2) appraise and document whether or not the automated security tools produce the expected results**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **3) use the available security analysis tools appropriate to the defined information system to find security anomalies and document the results**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **4) interpret the results of automated security analysis**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **5) justify any suggested security relevant changes found by the tools and document the results**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **h. Application Security**
 - ▼ **1) appraise whether or not application security features produce the expected results and document the results**
 - ▼ *NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
 - ▼ **2) verify the presence of and the appropriate use of application security features, and document the results**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **i. Disaster Recovery Planning**
 - ▼ **1) verify the presence of a disaster recovery plan as documented in the SSAA**
 - ▼ *NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
 - ▼ **2) appraise the effectiveness of the disaster recovery plan as described in the SSAA**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
 - ▼ **3) document the results of this verification and appraisal**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **j. Change Control Policies**
 - ▼ **1) verify the implementation of the change control management processes**
 - ▼ *NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **2) verify the presence of change control policies as documented in the SSAA**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **3) document the results of this verification**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **k. Labeling**

▼ **1) verify and document that labeling is accomplished in accordance with the requirements documented in the SSAA**

▼ *NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **l. Marking of Media**

▼ **1) verify and document that all media in use is marked as appropriate, based on the requirements defined in the SSAA**

▼ *NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **m. Documentation Issues**

▼ **1) report conformance/non-conformance to the specified system certification documentation requirements**

▼ *NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **2) verify the presence of system standard operating procedures**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **3) verify that the SSAA has been validated from the DAA/CA perspective**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **4) verify that the appointment of personnel with any level of privileged access has been identified in writing, as required**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **5) verify the presence of documentation or a manual used by the system administrator (SA) and information system security officer (ISSO) to set up the system security configuration**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **n. Operating System Integrity**

- ▼ **1) demonstrate that the operating system integrity capabilities are present in the information system by incorporating operating system configuration management guidelines, including installin**

- ▼ *NO SUB-CATEGORY

- HSCJ 202

- MISM 670

- MISM 661

- ▼ **2) report the results of the ST&E pertaining to operating system integrity**

- ▼ NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ **3) verify that the operating system integrity capabilities present in the information system are managed and work as defined in the SSAA**

- ▼ NO SUB-CATEGORY

- HSCJ 202

- MISM 670

- MISM 661

- ▼ **o. Protecting From Malicious/Mobile Code**

- ▼ **1) use the available tools to test the system capabilities in order to identify residual risk**

- ▼ *NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ **2) verify that appropriate capabilities are resident in the system to mitigate risk from malicious/mobile code contamination**

- ▼ NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ **3) document the results of testing to support the system residual risk analysis**

- ▼ NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ **p. Coordination with Related Security Discipline**

- ▼ **1) report, when required, the results of related security discipline testing**

- ▼ *NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ **2) verify that there are countermeasures defined in the SSAA for physical security, personnel security, all aspects of INFOSEC, etc**

- ▼ NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ **q. Testing Implementation of Security Features**

- ▼ **1) test and verify the effectiveness of all security features, such as password aging and internal labeling, and document the results**

- ▼ *NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ 2) analyze the impact of the absence of security features that are necessary for secure systems operations, and categorize the residual risk

- ▼ NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ **8. DEVELOPING RECOMMENDATION TO DAA**

- ▼ **a. Access Control Policies**

- ▼ 1) explain the access control policies as implemented in the current system to the DAA

- ▼ *NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ 2) define who in the current system has access to information views, who grants the access authorization, and the parameters which will be used to validate access authorization

- ▼ NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ 3) identify the adequacy of the implemented access control mechanisms identified in the access control policy and comment on this in the report

- ▼ NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ 4) evaluate the access control mechanisms implemented in accordance with the policy, and include the results of this evaluation in the report

- ▼ NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ 5) recommend changes to the implemented access control mechanisms in the report as needed to meet requirements identified in the access control policies

- ▼ NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ **b. Administrative Security Policies and Procedures**

- ▼ 1) address all pertinent security policies and procedures not covered under the laws, agency-specific procedures, etc. (NOTE: this review examines these procedure

- ▼ *NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ 2) recommend administrative security policies and procedures to limit the impact of system technical security deficiencies

- ▼ NO SUB-CATEGORY

- HSCJ 202

- MISM 661

- ▼ **c. Certification**

- ▼ **1) recommend the conditions upon which an accreditation decision is to be made, including the technical evaluation of security features, as well as other safeguards**
 - ▼ *NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **2) identify the deficiency and alternative safeguards and procedures that could be employed to limit the impact of system deficiency**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **3) recommend the adoption of requirements which were previously unspecified, but which may be crucial to secure deployment and operation of the system**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **4) report on the comprehensive evaluation of the technical and non-technical security features of the IS and other safeguards, to meet the security and accreditation requirement**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **d. Roles and Responsibilities**
 - ▼ **1) outline current roles and responsibilities of personnel assigned access to the systems being certified**
 - ▼ *NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
 - ▼ **2) recommend changes to include additions for improving the roles and responsibilities and accountability for personnel with various levels of access to the information systems being c**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **e. Brief and Defend ST&E Results**
 - ▼ **1) describe the ST&E results**
 - ▼ *NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
 - ▼ **2) explain and defend the specific findings, including risk analysis/mitigation**
 - ▼ NO SUB-CATEGORY
 - HSCJ 202
 - MISM 661
- ▼ **f. Communicate Results of ST&E**
 - ▼ **1) render the technical findings into comprehensible language for non-technical managers**
 - ▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ 2) **communicate the results/findings to technical personnel who would be responsible for correcting the findings**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **g. Identify Potential Corrective Approaches**

- ▼ 1) **identify potential avenues of corrective action**

- ▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ 2) **provide corrective approaches to the DAA as potential mitigating factors, if adopted**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ 3) **address the technical aspects of the system to meet the technical security requirements for its intended use and to identify those areas where non-technical means such**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ 4) **restrictions are needed to reduce the risk of operating the system to an acceptable level**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **h. Determine Residual Risk**

- ▼ 1) **report the findings and the overall level of residual risk in the current system**

- ▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ 2) **compare and contrast the non-technical and technical test/evaluation results, the impact of any countermeasures, and determine the residual risk**

- ▼ NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ **9. COMPLIANCE VALIDATION**

- ▼ **a. Automated Tool**

- ▼ 1) **conduct post-accreditation periodic compliance validation reviews in accordance with the timelines identified in the SSAA or as requested by the DAA**

- ▼ *NO SUB-CATEGORY

HSCJ 202

MISM 661

- ▼ 2) **identify and discuss the testing tools with site personnel, if necessary**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **3) verify that the identified tools remain compliant with the current accreditation**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **b. Process Review**

▼ **1) discuss the identified life-cycle processes and procedures with cognizant site personnel**

▼ *NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **2) identify the life-cycle processes and procedures to support mission accomplishment**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **3) manage the review in accordance with the identified timelines**

▼ NO SUB-CATEGORY

HSCJ 202
ISYS 411
MMBA 640
MISM 661

▼ **4) review the physical, environmental, technical, and procedural security disciplines**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **5) review the SSAA and assist in its revision, if necessary**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **6) verify that the identified life-cycle processes and procedures remain compliant with the current accreditation**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **7) verify the status of the system's current risks**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **8) explain the results and the recommendations, based on the findings, in support or denial of continued certification to the DAA**

▼ NO SUB-CATEGORY

HSCJ 202
MISM 661

▼ **c. Connection Requirements**

- ▼ **1) verify that connections of systems to networks or to each other follow a defined set of requirements as found in the SSAA.**

▼ *NO SUB-CATEGORY

HSCJ 202
MISM 661

b. Standard Specifications

UNCLASSIFIED

NSTISSI No. 4015
December 2000



National Training Standard
for
System Certifiers

THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER
INFORMATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY.

UNCLASSIFIED

UNCLASSIFIED



National Security Telecommunications and Information Systems Security Committee

FOREWORD

1. This instruction establishes the minimum course content or standard for the development and implementation of education and training for System Certifier professionals in the disciplines of telecommunications security and information systems (IS) security. Please check with your agency for applicable implementing documents.
2. Representatives of the National Security Telecommunications and Information Systems Security Committee may obtain additional copies of this NSTISSI at the address listed below.
3. U.S. Government contractors and vendors shall contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.

MICHAEL V. HAYDEN
Lieutenant General, USAF

NSTISSC Secretariat (I42), National Security Agency, 9800 Savage Road STE 6716, Ft Meade MD 20755-6716
(410) 854-6805, U.FAX: (410) 854-6814
nstissc@radium.ncsc.mil

UNCLASSIFIED

National Training Standard for System Certifiers

SECTION

PURPOSE **I**
APPLICABILITY **II**
RESPONSIBILITIES..... **III**
PREFACE **IV**

SECTION I - PURPOSE

1. This instruction and the attached ANNEXES establish the minimum education and training standard for the development and implementation of education and training for System Certifiers in the disciplines of telecommunications and information systems (IS) security.

SECTION II - APPLICABILITY

2. National Security Telecommunications and Information Systems Security Directive (NSTISSD) No. 501 establishes the requirement for federal departments and agencies to implement training programs for information systems security (INFOSEC) professionals. As defined in NSTISSD No. 501, an INFOSEC professional is an individual responsible for the security oversight or management of national security systems during phases of the life-cycle. That directive is being implemented in a synergistic environment among departments and agencies committed to satisfying these INFOSEC education and training requirements in the most effective and cost efficient manner possible. This instruction is the continuation of a series of minimum training and education standards being developed to assist departments and agencies in meeting their responsibilities in these areas (NSTISSI Nos. 4011, 4012, 4013 and 4014). Concomitant capabilities required by the System Certifiers to perform the job functions competently are provided in ANNEX B of this instruction. The definitions for terminology used in this instruction are derived from the National INFOSEC Glossary, NSTISSI No. 4009. The references pertinent to this instruction, as well as other documents which can be used in conjunction with it, are listed in ANNEX C.

3. The body of knowledge required by this instruction may be obtained from a variety of sources, i.e., Defense Information Systems Agency (DISA), National Ssecurity Agency (NSA), and Government contractors, as well as from adaptations of existing department/agency education and training programs, or from a combination of experience and formal training. ANNEX A lists the minimal INFOSEC performance standard for a System Certifier.

4. This instruction is applicable to all U.S. Government departments and agencies as well as Government contractors responsible for the development and implementation of education and training for telecommunications and IS security System Certifiers.

SECTION III - RESPONSIBILITIES

5. Heads of U.S. Government departments and agencies shall ensure System Certifiers (or their equivalents) are made aware of the body of knowledge outlined in this

instruction, and provide such education and training to those requiring it at the earliest practicable date.

6. The National Manager shall:
 - a. maintain and provide an INFOSEC education and training standard for System Certifiers to U.S. Government departments and agencies;
 - b. ensure appropriate INFOSEC education and training courses for System Certifiers are developed; and
 - c. assist other U.S. Government departments and agencies in developing and/or conducting INFOSEC education and training activities for System Certifiers as requested.

SECTION IV - PREFACE

7. The System Certifier is an individual or a member of a team who performs the comprehensive multidisciplined assessment of the technical and non-technical security features and other safeguards of an information system in an operational configuration, made in support of the accreditation process. The Certifier identifies the assurance levels achieved in meeting all applicable security policies, standards, and requirements for the Designated Approving Authority (DAA), who in turn determines whether or not an information system and/or network is operating within the bounds of specified requirements and at an acceptable level of risk. For the purposes of this document, we have defined "System Certifier" to avoid any confusion between it and the Department of Defense definition of "certification authority," as well as the NSTISSC definition of "certification agent." In this document, the term "System Certifier" is used as defined above.

8. The designated Certification Authority (sometimes referred to as "certification agent," as defined in NSTISSI No. 4009) is ultimately responsible for determining the correct skill sets required to adequately certify the system, and for identifying personnel to accomplish the comprehensive evaluation of the technical and non-technical security features of the system. The scope and the complexity of the information system determine whether the Certifier will be an individual or a member of a team performing the certification. The Certifiers' responsibilities evolve as the system progresses through the life-cycle process. Because an in-depth understanding and application of the certification and accreditation (C&A) process is required of the System Certifiers, these professionals operate at the highest level of the Information Technology Security Learning Continuum model referenced in the National Institute of Standards and Technology (NIST) Special Publication No. 800-16. According to this model, learning starts with awareness, builds to training, and evolves into education, the highest level. Overall the performance items contained in this training standard are at that advanced level.

9. To be a qualified System Certifier, one must first be formally trained in the fundamentals of INFOSEC, and have field experience. It is recommended that System Certifiers have system administrator and/or basic information system security officer (ISSO) experience, and be familiar with the knowledge, skills and abilities (KSAs) required of the DAA. Throughout the complex information systems certification process, the Certifiers exercise a considerable amount of INFOSEC-specific as well as non-INFOSEC-specific KSAs. ANNEX A lists the actual performance items under each of the System Certifier

KSAs, which in turn are outlined under each of the major job functions. Concomitant capabilities, provided in ANNEX B, are those capabilities which are exercised while performing a specified Certifier job function.

10. While this Instruction was developed using the National Information Assurance Certification and Accreditation Process (NIACAP) as a framework, this training standard employs common knowledge, skill, and attribute requirements that can be extended to develop courseware for any certification and accreditation process.

UNCLASSIFIED

ANNEX A

MINIMAL INFOSEC PERFORMANCE STANDARD FOR SYSTEM CERTIFIERS

Job Functions Using Competencies Identified In:

NSTISSI 1000, National Information Assurance Certification and Accreditation Process (NIACAP)

DoD Instruction 5200.40, DoD Information Technology (IT) Security Certification and Accreditation (C&A) Process (DITSCAP)

NCSC-TG-029, Version 1, Introduction to Certification and Accreditation

FIPS Publication 102, Guideline for Computer Security Certification and Accreditation

NCSC-TG-031, Certification and Accreditation Process Handbook for Certifiers

1942-TR-002, Version 1, Accreditor's Guideline

SC-2610-143-93, DoD Intelligence Information Systems (DoDIIS) Site Certifier's Guide

DoDIIS Security Certification and Accreditation Guide

Job Functions

The INFOSEC functions of System Certifiers are performed during the following phases of the certification process:

1. Documenting Mission Need

The System Certifiers need to develop a comprehensive understanding of the mission and the functional responsibilities in order to ensure the success of the C&A processes. Certifiers must possess a global understanding of the C&A process, the system, and the mission it supports.

2. Conducting Registration

Registration involves the collection of information needed to address the certification process in a repeatable, understandable, and effective manner. These tasks involve gathering information to determine the security requirements and the level of effort necessary to accomplish C&A. The level of effort is influenced by the degree of assurance needed in the areas of confidentiality, integrity, accountability, and availability. Certifiers must consider the mission, environments, system life-cycle, existing documentation, risk, architecture, users, data classifications, external interfaces, etc.

3. Performing Negotiation

Negotiation is involved in every facet of the C&A process. Given the potentially large numbers of people and functional organizations involved, Certifiers must draw upon many sub-disciplines and roles to accomplish this mission. To this end, Certifiers must possess broad, well-developed negotiation skills. Negotiation skills are especially important for determining methodologies, defining the scope of the certification process, and acquiring the resources necessary to support the mission. Effective written and oral communication skills, flexibility, creativity, political acumen, and objectivity all contribute to effective negotiation activities.

UNCLASSIFIED

4. Preparing the System Security Authorization Agreement (SSAA)

Certifiers are part of a team composed of the Certification Authority, the program sponsor, a threat specialist, and others. This team prepares the SSAA, a document that describes the planned operating condition of the system being certified and the expected residual risk in operating the system. The Designated Approving Authority (DAA) approves the SSAA and the system is then implemented with the security requirements that have been determined for it. It is important to note that the SSAA is a living document, and as such will require periodic maintenance throughout the life-cycle management of the system.

5. Supporting Systems Development

During the systems development phase of a system certification, the Certifiers are responsible for evaluating the design of the system and ensuring that the security requirements are being properly addressed and satisfied. The specific activities are a function of the overall program strategy, the life-cycle management process, and the position of the information system in the life-cycle. As in the Certification Analysis phase, the system development activities ensure that the requirements of the SSAA are followed during each life-cycle phase of the development and modification of the information system.

6. Performing Certification Analysis

Certification Analysis is the process of interacting with the system developer or owner/operator, and reviewing the documentation to carefully assess the functionality of the developing system, ensuring that it meets the security requirements as defined for its users, environment, connectivity, and other technical and non-technical factors in the SSAA.

7. Certification Evaluation

Security certification evaluation is the process whereby the Certifiers verify and validate through formal security testing and evaluation (ST&E), that the implementation of the information system (IS) complies with the technical and non-technical security requirements stated in the SSAA, and that any observed deficiencies are fully documented and presented to the DAA for consideration in the accreditation decision.

8. Developing Recommendation to the DAA

The Certifiers prepare appropriate documentation regarding all findings resulting from the ST&E, and recommends to the DAA the degree to which the evaluated system satisfies all the defined security requirements. In addition, this documentation offers the Certifier's opinion concerning any identified residual risk that may preclude accreditation of the system for operation.

9. Compliance Validation

The Certifier's focus during this phase is the audit of the accredited IS, which is operating under the approval of the DAA, who has accepted any identified residual risk. Therefore, the Certifiers audit operations to ensure they remain consistent with the DAA-accepted level of risk.

10. Maintenance of the SSAA

The Maintenance of the SSAA function involves determining whether or not any IS implementation changes that dictate a need to recertify the implementation of the IS will require an update of the SSAA. If changes occur that dictate a need for a recertification effort, then the Certifier functions as defined in the C&A process are again performed for these changes, or for

UNCLASSIFIED

the entire IS as necessary. Additionally, Certifiers must ensure that the recertification effort is reported to the DAA for continued approval to operate.

Terminal Objective:

Given an information system, the System Certifiers will explain and apply a recognized methodology leading to the security certification of that system in accordance with a prescribed set of criteria (i.e., the International Common Criteria), and provide an accreditation recommendation to the DAA for consideration in the accreditation decision. To be acceptable, the certification must be performed in accordance with applicable INFOSEC regulations, policies and guidelines.

List of Performance Items Under Competencies

In each of the competency areas listed below, the System Certifiers shall perform the following functions:

1. DOCUMENTING MISSION NEED

a. Knowledge and/or Awareness of Security Laws

- 1) identify relevant nation-state security laws, treaties, and/or agreements;
- 2) interpret nation-state security laws, treaties, and/or agreements in relation to mission accomplishment;
- 3) relate the identified nation-state security laws, treaties, and/or agreements to the mission needs;
- 4) discuss identified nation-state security laws, treaties, and/or agreements with involved site personnel; and
- 5) explain interpretation in support or denial of certification to involved site personnel.

b. Coordination with Related Disciplines

- 1) identify the related disciplines required for accomplishing the IS certification; and
- 2) discuss mission-specific discipline relationships and IS requirements with involved site personnel.

c. Understand Mission

- 1) study the mission critical elements, to include system mission, functions, and system interfaces;
- 2) verify that mission critical elements are completely identified (e.g., operational procedures and classification requirements);
- 3) confirm the mission description is complete as it relates to documented IS needs, to include system life cycle;
- 4) discuss the interpretation of mission critical elements in support or denial of certification with involved site personnel; and

UNCLASSIFIED

5) research and discuss mission operational environment (e.g., charter, scope of authorities, activation call-up procedures, Information Warfare Condition (INFOCON) processes).

d. Contingency Planning

- 1) assess the need for contingency planning;
- 2) study the identified critical contingency elements;
- 3) confirm that the critical elements of mission contingency planning have been identified in relation to the specific operational environment;
- 4) discuss the critical contingency elements and IS requirements in relation to mission accomplishment to assure system recovery and reconstitution;
- 5) explain the appraisal in support or denial of certification to involved site personnel; and
- 6) verify that the documented mission need elements are identified in the critical system contingency plan.

2. CONDUCTING REGISTRATION

a. System Certification Memorandum of Understanding (MOU) or Other Instruments

- 1) propose the development of an MOU or other appropriate instruments;
- 2) describe the purpose, scope, and contents of a particular MOU or other instruments;
- 3) identify the respective parties and their roles;
- 4) discuss anticipated challenges to an MOU or other instruments;
- 5) explain the various details of an MOU or other instruments;
- 6) interpret the agreements specified in an MOU or other instruments;
- 7) use an MOU or other instruments to define the responsibilities and requirements for team members with specialized knowledge;
- 8) use an MOU or other instruments to assist in SSAA and other policy development;
- 9) comply with the requirements of a system certification MOU or other instruments;
- 10) verify the integrity of an MOU or other instruments; and
- 11) report the status of MOUs or other instruments to the DAA.

b. Collect Security Requirements

- 1) describe the security requirement collection process;
- 2) research security requirements; and
- 3) describe to the DAA, program management office (PMO), etc., the appropriate requirements for system security.

c. Knowledge and/or Awareness of Security Laws Required for System Being Evaluated

UNCLASSIFIED

- 1) explain the applicable laws, statutes, and regulations;
- 2) discuss how the system will operate according to legal mandates; and
- 3) identify the organizational point of contact for legal advice.

d. Audit Collection Requirements

and

- 1) describe the audit collection requirements relative to system certification;
- 2) assist in the identification of audit requirements.

e. Coordination with Related Disciplines

system;

certification of the system; and

- 1) discuss the role of related security disciplines in the overall protection of the
- 2) describe the related security disciplines and how they apply to the
- 3) identify the related disciplines needed for the certification team.

f. Configuration Control Policies

policy.

- 1) advise in the development of configuration control policies;
- 2) assess the system configuration control plan against policy; and
- 3) report to the DAA the deficiencies/discrepancies in the configuration control

g. Contingency Planning

- 1) assess the need for contingency planning;
- 2) propose contingency planning activities;
- 3) discuss the contingency planning process;
- 4) assess contingency planning; and
- 5) report to the DAA any discrepancies or deficiencies in contingency plans.

h. Personnel Selection

skills for the IS involved.

- 1) explain the criteria for personnel selection for the certification team; and
- 2) perform personnel selection for the certification team based on the requisite

i. Roles and Responsibilities

and

members.

- 1) identify and define the roles and responsibilities of the certification team;
- 2) propose the roles and responsibilities of individual certification team

j. Scope and Parameters of the Certification

UNCLASSIFIED

describe, define, and present the scope and parameters of the certification.

k. Set Certification Process Boundaries

- 1) define and describe the certification process boundaries; and
- 2) identify and propose the boundaries of the certification process.

l. Risk Management

- 1) select the appropriate risk management methodology for the IS to be certified;
- 2) discuss the risk management methodology and threat mitigation using examples and explanations; and
- 3) describe the risk management methodology appropriate to the certification of the system.

m. System Description

verify that the system description is consistent with the documented mission need.

n. System Security Policy

- 1) ensure the development and inclusion of a comprehensive system security policy; and
- 2) assess policy to ensure it conforms with applicable laws and directives and data owner requirements.

o. Budget/Resources Allocation

- 1) define and describe budget elements related to the certification process; and
- 2) identify the resource requirements necessary to accomplish the certification process.

p. Timeline/Scheduling

- 1) establish certification milestones; and
- 2) relate the milestones to roles and responsibilities.

q. Life-Cycle System Security Planning

- 1) assess life-cycle security planning against requirements, directives and laws;
- 2) describe life-cycle security planning; and
- 3) assist in life-cycle security planning with respect to the certification requirements.

UNCLASSIFIED

3. PERFORMING NEGOTIATION

a. Life-Cycle System Security Planning

- 1) explain life-cycle system security planning;
- 2) propose life-cycle system security attributes to involved site personnel; and
- 3) propose improvements to the plans developed by site personnel.

b. Set Certification Process Boundaries

- 1) discuss setting certification boundaries;
- 2) describe setting certification boundaries;
- 3) influence certification boundaries;
- 4) justify setting certification boundaries; and
- 5) report the setting of certification boundaries as part of the SSAA.

c. Risk Management

appraise elements of life-cycle activity versus the risk management process components of mission, vulnerabilities, threat, and countermeasures to determine if system development activity is ready for certification.

d. Knowledge and/or Awareness of Security Laws

use the knowledge and awareness of security laws to ensure system development activities follow legal guidelines.

4. PREPARING SSAA

a. Access Control Policies

- 1) categorize access control policies;
- 2) describe access control policies; and
- 4) relate access control policies to appropriate "umbrella" guidance and policies.

b. Security Policies and Procedures

- 1) define and understand the topics that security policies and procedures must address as part of the certification process;
- 2) discuss the impact of policy and procedures on risk and operations;
- 3) explain how the system operating policies and procedures define the implementation of the security requirements;
- 4) integrate the identified security policies and procedures (i.e., audit policies, access control policies) as minimum requirements into the ST&E plan;
- 5) interpret the relationship between security policy and procedures and the security requirements;

UNCLASSIFIED

- 6) assist the DAA, program manager (PM), and user in understanding the security policies and procedures; and
- 7) describe the security solutions and implementations that meet the specified system security requirements.

c. Documentation Policies

- 1) identify documentation policies that apply to the preparation of the SSAA;
- and
- 2) ensure that the appropriate documentation policies are followed in preparing the SSAA.

d. Requirements Derivation

- 1) categorize security certification requirements;
- 2) discuss how technical and non-technical security requirements are derived;
- 3) identify requirements that are applicable to the system under certification and accreditation;
- 4) identify the source of the security requirements;
- 5) identify the source of the security requirements for use during negotiations, development of the SSAA, and compliance validation;
- 6) interpret security requirements for the specific mission, environment, data classification level, and architecture;
- 7) summarize the security requirements and construct a requirements traceability matrix (RTM);
- 8) use security requirements to assist in the development of ST&E plans;
- 9) verify that security certification requirements are included in the ST&E plan; and
- 10) explain the security requirements in order to develop a common understanding among the DAA, PM, and Certification Authority.

e. Understand Mission

- 1) describe the system mission focusing on the security relevant features of the system required for the SSAA;
- 2) discuss the purpose of the system and its capabilities in the SSAA;
- 3) explain the impact of the mission statement on security requirements;
- 4) summarize the mission and prepare a summary for the SSAA; and
- 5) use the mission statement to identify applicable security certification requirements in the SSAA.

f. Security Domains

- 1) identify any specific security domains as they apply to the system mission and function; and
- 2) relate the interactions between different security domains in support of the system mission and functions.

UNCLASSIFIED

g. System Description

- 1) appraise the system concept of operations (CONOPS);
- 2) assess the system's criticality and its impact on the level of risk that is acceptable;
- 3) define the system user's characteristics and clearances;
- 4) define the security clearances of the user population and the access rights to restricted information;
- 5) define the type of data and data sensitivity;
- 6) describe the system CONOPS and security CONOPS in the SSAA;
- 7) describe the system criticality in the SSAA;
- 8) describe the system functions and capabilities;
- 9) examine the mission to determine the national security classification of the data processed;
- 10) identify the system acquisition strategy and system life-cycle phase; and
- 11) use the data sensitivity and labeling requirements to determine the system classification.

h. Environment and Threat Description

- 1) derive the system operating environment and threat descriptions from the mission documentation; and
- 2) prepare a description of potential threats based upon an analysis of the operating environment, and the system development environment for inclusion in the certification reports for the DAA.

I. System Operating Environment

- 1) describe the administrative security procedures appropriate for the system being certified;
- 2) analyze the physical environment in which the system will operate; address all relevant parts of the system's environment, including descriptions of the physical, administrative, developmental, and technical areas; describe any known or suspected threats specifically to be considered for the described environment;
- 3) describe the security features that will be necessary to support site operations (the physical security description should consider safety procedures for personnel operating the equipment);
- 4) identify maintenance procedures needed to ensure physical security protection against unauthorized access to protected information or system resources;
- 5) identify procedures needed to counter potential threats that may come from inside or outside of the organization;
- 6) identify the physical support features of the facility, including air conditioning, power, sprinkler system, fences, and extension of walls from true-floor to true-ceiling construction, sensitive space, work space, and the building;
- 7) determine if training procedures match the users' levels of responsibility, and provide information on potential threats and how to protect information; and
- 8) identify aspects of physical security, such as a defined secure work area; the means used to protect storage media (e.g., hard drives and removable disks); protecting access to workstation ports (e.g., communication ports); a controlled area for shared resources (e.g.,

UNCLASSIFIED

databases and file servers); and the means of protection used for cable plant and communication hubs and switches which are used to connect workstations and shared resources.

j. System Development, Integration, and Maintenance Environment

- 1) describe the system development approach and the environment within which the system will be developed and maintained;
- 2) describe the information access and configuration control issues for the system; and
- 3) determine the appropriate types of system development and maintenance environments.

k. Threat Description and Risk Assessment

- 1) define, in conjunction with the system owner, the potential threats that can affect the confidentiality, integrity, and availability of the system; clearly stating the nature of the threat that is expected, and where possible, the expected frequency of occurrence;
- 2) identify threats, such as penetration attempts by hackers, damage or misuse by disgruntled or dishonest employees, and misuse by careless or inadequately trained employees;
- 3) identify unintentional human error, system design weaknesses, and intentional actions on the part of authorized, as well as unauthorized users that can cause these events; and
- 4) describe insider threat, including the good intentions of a trusted employee who circumvents security in order to accomplish the job.

l. System Architectural Description

- 1) describe the accreditation boundary of the system;
- 2) describe the system architecture including the configuration of any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information that includes computers, ancillary equipment, software, firmware, and similar procedures and services, including support services and related resources;
- 3) describe the system's internal interfaces and data flows;
- 4) identify and describe the system's external interfaces and the relationship between the interfaces and the system;
- 5) describe the proposed and appropriate hardware and its function (**NOTE:** hardware is the physical equipment, as opposed to programs, procedures, rules, and associated documentation);
- 6) describe the proposed and appropriate software and its intended use (**NOTE:** software includes the entire set of application programs, software procedures, software routines, and operating system software associated with the system; this includes manufacturer-supplied software, other commercial off-the-shelf software, and all program-generated application software);

UNCLASSIFIED

7) determine the types of data and the general methods for data transmission
(NOTE: if specific transmission media or interfaces to other systems are necessary, these needs may influence the security requirements for the system);

8) develop an overview of the internal system structure including the anticipated hardware configuration, application software, software routines, operating systems, remote devices, communications processors, networks, and remote interfaces;

9) develop diagrams or text to explain the flow of critical information from one component to another;

10) identify and include diagrams or text that clearly delineate the components that are to be evaluated as part of the C&A task;

11) identify components which are not to be included in the evaluation; and

12) prepare a high level overview of the types of hardware, software, firmware, and associated interfaces envisioned for the completed system.

m. Identify C&A Organizations and Resources

1) enlist the assistance of a contractor team or other government organizations
(NOTE: the CA has the responsibility to form the team, coordinate the C&A activities, conduct the analysis, and prepare or validate the SSAA);

2) identify the appropriate statutory authorities, and the resource and training requirements necessary to conduct the certification;

3) identify the organizations, individuals, and titles of the key authorities involved in the C&A process;

4) determine the certification team's roles and responsibilities;

5) form the C&A team after the CA knows the certification level and tasks required;

6) identify the roles of the certification team members as needed and their responsibilities; and

7) include team members who have composite expertise in the whole span of activities required, and who are independent of the system developer or PM.

n. Tailor the Agency-specific C&A Guidelines (e.g., NIACAP, DITSCAP) and Prepare the C&A Plan

1) adjust and document the C&A guideline (e.g., NIACAP, DITSCAP) activities to fit the program strategy;

2) conduct a review of the C&A guideline plan and SSAA by the DAA, CA, PM, and user representative;

3) determine the skills needed to perform the analysis and the supporting documentation;

4) prepare a process diagram of the system life-cycle activities and identify the current phase of life-cycle activity;

5) schedule the C&A guideline activities to meet the system schedule (for example, if the system has already completed preliminary design, all C&A guideline phase one activities should be completed as soon as possible);

6) tailor the C&A process as agreed upon in the SSAA;

7) tailor the C&A guideline process to the system life-cycle at the current system phase or activity;

8) tailor the process to the incremental development strategy (if one is used);

UNCLASSIFIED

9) tailor the security activities to system development activities to ensure that the security activities are relevant to the process and provide the required degree of analysis;

10) determine the appropriate certification analysis level and adjust the C&A guideline activities to the program strategy and system life-cycle;

11) determine where to focus the analysis and testing; and

12) identify the appropriate level of effort.

o. Prepare SSAA Added Material

1) consolidate documentation, drawing together all pertinent materials into a logical, sequential, and coherent document which will support the DAA's decision to approve or disapprove;

2) identify constraints, assumptions, and dependencies of the C&A process being implemented; and

3) identify the conditions under which certification activities were accomplished.

p. Requirements Traceability

1) develop the security certification test plan documentation;

2) develop the ST&E evaluation report documentation;

3) identify the source of the security requirements for use during negotiations, development of the SSAA, and compliance validation;

4) specify the required security evaluation documentation;

5) use security requirements to develop the ST&E plans and procedures;

6) develop security certification test procedures; and

7) outline any unique certification analysis documentation requirements.

5. SUPPORTING SYSTEMS DEVELOPMENT

a. Coordination with Related Disciplines

1) explain to the development team and to the accreditor the need for coordination with related disciplines;

2) perform coordination with the various offices responsible for the related disciplines; and

3) verify coordination with related security disciplines, e.g., physical, emanations, personnel, operations, and cryptographic security.

b. Configuration Control

1) appraise current system configuration control;

2) discuss configuration control with the development team for compliance with required INFOSEC policy and technology;

3) propose configuration control changes;

4) report the configuration control deficiencies to the developer; and

UNCLASSIFIED

5) verify that the activities associated with configuration control, i.e., physical and functional audits, inventory of the hardware and software components, etc., are adequately documented and performed.

c. Information Security Policy

1) identify applicable information security policy;
2) explain information security policy to the development team for the secure operation of the system; and
3) use information security policy to ensure the appropriate secure operation of the system.

d. Life-Cycle System Security Planning

1) appraise the life-cycle system security planning proposed by the development team;
2) assist with the information security planning for life-cycle system security;
3) explain the life-cycle system security planning to the development team;
4) influence the development team's approach to life-cycle system security planning; and
5) verify that life-cycle system security planning has been accomplished.

e. Parameters of the Certification

1) propose alterations to the parameters of the certification process as the system development progresses and the design is modified;
2) compare the parameters of the certification to those of similar systems or during parallel certification;
3) determine the parameters of the certification to ensure mission accomplishment;
4) explain the parameters of the certification to system developers and maintainers;
5) use the parameters of the certification; and
6) verify adherence to the parameters of the certification.

f. Principles and Practices of Information Security

1) understand the principles and practices of information security;
2) identify principles and practices of information security that pertain to the certification;
3) adhere to recognized principles and practices of information security; and
4) explain the principles and practices of information security that pertain to the certification to the developers.

g. Network Vulnerabilities

1) identify any network vulnerabilities for the system developers and maintainers;

UNCLASSIFIED

- 2) demonstrate to the system developers and maintainers the network vulnerabilities that are present during the development of the system;
- 3) evaluate the impact of network vulnerabilities;
- 4) explain unacceptable network vulnerabilities to the developers;
- 5) respond to network vulnerabilities by suggesting corrective measures when possible; and
- 6) stay current on network vulnerabilities.

h. Security Engineering

- 1) assist developers and maintainers with system security engineering principles as required for information security and certification and accreditation;
- 2) define security engineering principles that are applicable to information security;
- 3) explain security engineering principles and practices;
- 4) review security engineering principles and practices for compliance with information security policies; and
- 5) outline best security engineering practices as defined by the National Information Assurance Partnership (NIAP).

i. Access Control Policies

- 1) be aware of access control policies;
- 2) evaluate for the developers and maintainers the strengths and weaknesses of access control policies;
- 3) explain the need for access control policies;
- 4) identify to the developers and maintainers access control policies that are applicable to information security; and
- 5) recommend access control policy changes that are appropriate for the system being certified.

6. PERFORMING CERTIFICATION ANALYSIS

a. Access Control

- 1) appraise access control privilege assignment;
- 2) appraise access controls defined as appropriate for the IS under review for subjects (e.g., local and remote users and/or processes);
- 3) appraise access controls for objects (e.g., data, information, and applications);
- 4) appraise access controls for privileged users and/or processes;
- 5) appraise management of the access control tables and lists;
- 6) appraise identification and authentication mechanisms which identify users and/or processes;
- 7) appraise the implementation of user privileges and group management assignments;
- 8) appraise managed and default file permission settings and factory settings;
- 9) appraise the effectiveness of password management implemented to enforce policies and procedures;

UNCLASSIFIED

- 10) appraise whether the identification and authentication mechanism can correctly identify users and/or processes;
- (DAC/MAC);
- 11) identify the requirement for discretionary/mandatory access controls
- 12) explain to other team members and managers how access privileges are set;
- 13) match data ownership and responsibilities with access control rights;
- 14) match the requirements for respective access control features with appraised controls implemented;
- 15) match the access control requirements with user roles and group management;
- 16) determine the security countermeasures to implement effective access control;
- 17) verify the contents of the user registry and access control tables;
- 18) verify the effectiveness of password management software in enforcing policies and procedures;
- 19) identify representative processes which must use an appropriate identification and authentication mechanism;
- 20) propose the security test and evaluation plan/procedures and schedule to test and evaluate agreed upon security countermeasures for access control; and
- 21) report recommended changes to the implemented access control mechanisms as needed to meet the requirements identified in the access control policies.

b. Audits

- 1) appraise the system's ability to produce viable, inclusive audit data for review and analysis (e.g., selection capabilities for review of audit information);
- 2) appraise the alert capabilities provided by audit/intrusion detection tools;
- 3) verify the criteria for generating alerts provided by audit/intrusion detection tools;
- 4) appraise the availability of audits including recovery from permanent storage;
- 5) appraise the identification of anomalies which indicate successful violation/bypass of security capabilities;
- 6) appraise the inherent audit capabilities and the proposed implementation;
- 7) appraise the processes for analyzing audit information;
- 8) appraise the report generation capability;
- 9) appraise the use of audit information to identify attempts to violate/bypass the proper operation of system security capabilities;
- 10) appraise the use of audit information to validate the proper operation of automated system security capabilities;
- 11) identify the audit elements and capabilities available on the system being evaluated;
- 12) identify the audit event characteristics and their granularity (i.e., type of event, success/failure, date/time stamp, user ID);
- 13) summarize the data which supports trend analysis;
- 14) verify that the audit elements capture information that meets specified security requirements;
- 15) verify that the audit log overflow policy is correctly implemented;
- 16) verify that audit procedures exist to implement the policy (i.e., data reviews, audit retention and protection, response to alerts, etc);

UNCLASSIFIED

- 17) verify that audit processes support interpretation of the audit data;
- 18) verify that the audit retention capability meets the system security requirements;
- 19) verify that protections are in place to prevent the audit trails from being modified by any means, including direct edits of media or memory;
- 20) report the audit collection requirements to meet a stated authorization policy;
- 21) report any alternative means to satisfy the audit collection requirements;
- 22) propose aperiodic security test and evaluation plans and procedures to test and evaluate agreed upon audit functionality and events;
- 23) verify that system resources are sufficient to log all required events;
- 24) interpret the audit policy to be implemented (to include which events are to be recorded, what action should occur when the log fills, how long audits are to be retained, etc.);
- 25) determine the impact of audit requirements on the system operation requirements; and
- 26) appraise the capabilities of the add-on audit analysis and intrusion detection tools that are implemented.

c. Applications Security

- 1) appraise the effectiveness of applications security mechanisms and their interactions with other systems and network security mechanisms;
- 2) differentiate between the operating system and application system security features; and
- 3) propose security test and evaluation plans and procedures to test and evaluate agreed upon security countermeasures provided by application security mechanisms.

d. Confidentiality, Integrity and Availability (CIA)

- 1) explain the stated system requirements for confidentiality, integrity, and availability in the system design/SSAA documentation;
- 2) appraise the network architecture and what security mechanisms are used to enforce the CIA security policy; and
- 3) appraise the network security posture in light of the CONOPS and the abilities of the expected users and system administrators.

e. Countermeasures

- 1) appraise the requirements for additional countermeasures based on the security policy being implemented (e.g., routers, firewalls, guards, intrusion detection devices);
- 2) study the security countermeasures documented in the SSAA; and
- 3) propose security test and evaluation plans and procedures to test and evaluate agreed upon security countermeasures documented in the SSAA.

f. Documentation

- 1) identify the documentation of security-related function parameters, defaults and settings;

UNCLASSIFIED

- 2) report the review of the documentation, noting the adequacy of detail; and
- 3) identify the deficiencies in the system documentation, whether they be missing documents or inadequate detail in the existing documentation.

g. Network Security

- 1) appraise the network connectivity policy and the proposed implementation for connection;
- 2) appraise the security requirements for interconnectivity with other systems/networks;
- 3) verify that formal approvals have been granted for other systems and networks for which interconnectivity is sought;
- 4) appraise the security attributes of both the data and users accessing the connected system to determine whether additional security requirements result; and
- 5) propose security test and evaluation plans and procedures to test and evaluate agreed upon security countermeasures for network connectivity.

h. Maintenance Procedures

appraise the proposed system maintenance and upgrade procedures to ensure that they comply with configuration management procedures (e.g., remote software updates).

i. Operating System Security

- 1) appraise the documentation and system configuration of security function defaults and settings, ensuring that all inappropriate factory defaults have been changed;
- 2) appraise how the system handles error conditions;
- 3) appraise the system recovery capability during loss of power situations;
- 4) assess and report any variance between documented and actually installed software and operating systems;
- 5) propose security test and evaluation plan/procedures to test and evaluate agreed upon security countermeasures enforced by the operating system;
- 6) verify that capabilities are employed to enforce the protection of the operating system by preventing programs or users from writing over system areas;
- 7) verify that protections are in place to prevent configuration files and pointers that can run in a supervisory state from unauthorized access or unauthorized modifications, deletions, etc.; and
- 8) verify that protections are in place to prevent the operating system kernel from being modified by any process, program or individual except through an approved organizational configuration management procedure.

j. Vulnerabilities

identify vulnerabilities inherent to the system's specific operating system, applications, and network configuration.

k. Contingency Operations

UNCLASSIFIED

- 1) appraise whether the disaster recovery mechanism adequately addresses the needs of the site;
- 2) appraise whether the plan sufficiently protects the security of the information and the investment made in life-cycle security processes;
- 3) match the requirements for disaster recovery/continuity of operation with mission requirements; and
- 4) match the requirements for emergency destruction procedures with mission requirements.

7. CERTIFICATION EVALUATION

a. Evaluation Techniques

- 1) use appropriate evaluation techniques, e.g., documentation review, automated tools, and written test plan and procedures, etc., in the conduct of the security test and evaluation;
- 2) choose the evaluation technique(s) to exercise and evaluate security countermeasures or capabilities documented in the SSAA; and
- 3) generate and/or validate the security test and evaluation plan and procedures.

b. Access Control

- 1) verify that access controls meet the criteria established in the SSAA;
- 2) document the results of the ST&E access control tests; and
- 3) describe the ST&E testing results for access controls.

c. Contingency Planning/Testing

- and
- 1) appraise the effectiveness of the contingency plan as described in the SSAA;
 - 2) document the effectiveness of the contingency plan.

d. Audit Trail

- deletion, and
- 1) demonstrate that the audit trail is secure from unauthorized alteration and
 - 2) document the results; and
 - 3) appraise whether the audit trail meets the requirements as defined in the SSAA and document the results.

e. Intrusion Detection

- 1) verify the presence of intrusion detection capabilities as defined in the SSAA and document the results;
- 2) demonstrate that the intrusion detection mechanisms work as outlined in the SSAA and document the results; and

UNCLASSIFIED

3) analyze the effectiveness of the intrusion detection capabilities and document the results.

f. Security Processing Mode

1) verify that the security processing mode has been identified;
2) justify any suggested change in the security processing mode, if found to be inadequate or inappropriate, and document the results; and
3) appraise whether or not the defined security processing mode is adequate for approving system certification, and document the results.

g. Automated Security Tools

1) identify appropriate security tools and document the results;
2) appraise and document whether or not the automated security tools produce the expected results;
3) use the available security analysis tools appropriate to the defined information system to find security anomalies and document the results;
4) interpret the results of automated security analysis; and
5) justify any suggested security relevant changes found by the tools and document the results.

h. Application Security

1) appraise whether or not application security features produce the expected results and document the results; and
2) verify the presence of and the appropriate use of application security features, and document the results.

i. Disaster Recovery Planning

1) verify the presence of a disaster recovery plan as documented in the SSAA;
2) appraise the effectiveness of the disaster recovery plan as described in the SSAA; and
3) document the results of this verification and appraisal.

j. Change Control Policies

1) verify the implementation of the change control management processes;
2) verify the presence of change control policies as documented in the SSAA;
and
3) document the results of this verification.

k. Labeling

verify and document that labeling is accomplished in accordance with the requirements documented in the SSAA.

UNCLASSIFIED

l. Marking of Media

verify and document that all media in use is marked as appropriate, based on the requirements defined in the SSAA.

m. Documentation Issues

- 1) report conformance/non-conformance to the specified system certification documentation requirements;
- 2) verify the presence of system standard operating procedures;
- 3) verify that the SSAA has been validated from the DAA/CA perspective;
- 4) verify that the appointment of personnel with any level of privileged access has been identified in writing, as required; and
- 5) verify the presence of documentation or a manual used by the system administrator (SA) and information system security officer (ISSO) to set up the system security configuration.

n. Operating System Integrity

- 1) demonstrate that the operating system integrity capabilities are present in the information system by incorporating operating system configuration management guidelines, including installing the latest patches and consulting with available experts and references, and by updating and testing these guidelines often;
- 2) report the results of the ST&E pertaining to operating system integrity; and
- 3) verify that the operating system integrity capabilities present in the information system are managed and work as defined in the SSAA.

o. Protecting From Malicious/Mobile Code

- 1) use the available tools to test the system capabilities in order to identify residual risk;
- 2) verify that appropriate capabilities are resident in the system to mitigate risk from malicious/mobile code contamination; and
- 3) document the results of testing to support the system residual risk analysis.

p. Coordination with Related Security Discipline

- 1) report, when required, the results of related security discipline testing; and
- 2) verify that there are countermeasures defined in the SSAA for physical security, personnel security, all aspects of INFOSEC, etc.

q. Testing Implementation of Security Features

- 1) test and verify the effectiveness of all security features, such as password aging and internal labeling, and document the results; and
- 2) analyze the impact of the absence of security features that are necessary for secure systems operations, and categorize the residual risk.

UNCLASSIFIED

8. DEVELOPING RECOMMENDATION TO DAA

a. Access Control Policies

- 1) explain the access control policies as implemented in the current system to the DAA;
- 2) define who in the current system has access to information views, who grants the access authorization, and the parameters which will be used to validate access authorization;
- 3) identify the adequacy of the implemented access control mechanisms identified in the access control policy and comment on this in the report;
- 4) evaluate the access control mechanisms implemented in accordance with the policy, and include the results of this evaluation in the report; and
- 5) recommend changes to the implemented access control mechanisms in the report as needed to meet requirements identified in the access control policies.

b. Administrative Security Policies and Procedures

- 1) address all pertinent security policies and procedures not covered under the laws, agency-specific procedures, etc. (**NOTE:** this review examines these procedures and policies in respect to applicable national laws and governing regulations consistent with security requirements); and
- 2) recommend administrative security policies and procedures to limit the impact of system technical security deficiencies.

c. Certification

- 1) recommend the conditions upon which an accreditation decision is to be made, including the technical evaluation of security features, as well as other safeguards;
- 2) identify the deficiency and alternative safeguards and procedures that could be employed to limit the impact of system deficiency;
- 3) recommend the adoption of requirements which were previously unspecified, but which may be crucial to secure deployment and operation of the system; and
- 4) report on the comprehensive evaluation of the technical and non-technical security features of the IS and other safeguards, to meet the security and accreditation requirement.

d. Roles and Responsibilities

- 1) outline current roles and responsibilities of personnel assigned access to the systems being certified; and
- 2) recommend changes to include additions for improving the roles and responsibilities and accountability for personnel with various levels of access to the information systems being certified.

e. Brief and Defend ST&E Results

- 1) describe the ST&E results; and

UNCLASSIFIED

- 2) explain and defend the specific findings, including risk analysis/mitigation.
- f. Communicate Results of ST&E
 - 1) render the technical findings into comprehensible language for non-technical managers; and
 - 2) communicate the results/findings to technical personnel who would be responsible for correcting the findings.
- g. Identify Potential Corrective Approaches
 - 1) identify potential avenues of corrective action;
 - 2) provide corrective approaches to the DAA as potential mitigating factors, if adopted; and
 - 3) address the technical aspects of the system to meet the technical security requirements for its intended use and to identify those areas where non-technical means such as procedures; or
 - 4) restrictions are needed to reduce the risk of operating the system to an acceptable level.
- h. Determine Residual Risk
 - 1) report the findings and the overall level of residual risk in the current system; and
 - 2) compare and contrast the non-technical and technical test/evaluation results, the impact of any countermeasures, and determine the residual risk.

9. COMPLIANCE VALIDATION

- a. Automated Tool
 - 1) conduct post-accreditation periodic compliance validation reviews in accordance with the timelines identified in the SSAA or as requested by the DAA;
 - 2) identify and discuss the testing tools with site personnel, if necessary; and
 - 3) verify that the identified tools remain compliant with the current accreditation.
- b. Process Review
 - 1) discuss the identified life-cycle processes and procedures with cognizant site personnel;
 - 2) identify the life-cycle processes and procedures to support mission accomplishment;
 - 3) manage the review in accordance with the identified timelines;
 - 4) review the physical, environmental, technical, and procedural security disciplines;
 - 5) review the SSAA and assist in its revision, if necessary;

UNCLASSIFIED

- 6) verify that the identified life-cycle processes and procedures remain compliant with the current accreditation;
- 7) verify the status of the system's current risks; and
- 8) explain the results and the recommendations, based on the findings, in support or denial of continued certification to the DAA.

c. Connection Requirements

verify that connections of systems to networks or to each other follow a defined set of requirements as found in the SSAA.

10. MAINTENANCE OF THE SSAA

a. Life-Cycle Security Planning

- 1) discuss, when consulted, proposed changes to the SSAA;
- 2) propose, where required, a need for recertification and reaccreditation; and
- 3) interpret, when consulted, changes that may affect the existing certification.

b. Documentation Policies

- 1) appraise the documentation policies for continued applicability;
- 2) identify the documentation policies for updates; and
- 3) verify changes against the original documentation policies.

c. Configuration Control/Change Management

- 1) appraise the configuration control for continued applicability;
- 2) identify the configuration control in place versus that which has been specified in the current SSAA;
- 3) list proposed changes to the previously approved system configuration and/or operating environment, to include system retirement;
- 4) analyze the above changes to determine if an assessment of the impact is required;
- 5) outline the process for an assessment of the impact of changes to the existing SSAA; and
- 6) revise the SSAA in accordance with the configuration changes.

d. Maintenance of Configuration Documents

- 1) appraise the maintenance of configuration documents; and
- 2) compare the maintenance of configuration documents for conformance to the SSAA.

e. Periodic Review of System Life-cycle

- 1) appraise the periodic review of the system/product life-cycle for conformance to the SSAA;

UNCLASSIFIED

- 2) initiate the periodic review of the system/product life-cycle for conformance to the SSAA; and
- 3) report on the periodic review of the system/product life-cycle.

f. Communicate Results

report the results of changes to the SSAA to the accreditor (DAA).

g. Convey Magnitude of Risk

identify the inherent and residual risks and the potential corrective approaches to the accreditor (DAA).

h. Brief and Defend ST&E Results

prepare and deliver the ST&E results to the accreditor (DAA).

ANNEX B

**CONCOMITANT CAPABILITIES
FOR SYSTEM CERTIFIERS**

These requirements do not imply that the System Certifiers need be an expert in these global and specific concomitant capabilities, but he or she must be qualified to discuss, explain, and employ them. The concomitant System Certifiers capabilities include but are not limited to the following:

GLOBAL CAPABILITIES:

administrative security
personnel security
physical security
communications security
network security
server security
client/workstation security
database security
application security
cryptographic key management
understanding how a system will be used, in
 what environment, and by whom
documentation
business background
computer science background
creativity in achieving solutions
creativity in functional solutions
decision-making and management skills
engineering background
flexibility
interpersonal skills
quick learner
ability to see the "big picture"
self-starter/motivated
ability to work well in a team
ability to think outside the box/system
ability to accept challenges
TEMPEST
INFOSEC
OPSEC
communication/writing skills
political skills

SPECIFIC CAPABILITIES:

acquisition and C&A processes
assessment and testing methodology
addressing client server security to evaluate
 that portion of the system
client/server security
vulnerability self-audit capabilities
 (analyzing the capabilities of the system
 system to detect changes and
 vulnerabilities)
ability to appraise the client/server security
 posture in light of the CONOPS
 and the abilities of the expected users and
 system administrators
configuration management processes
developing data flow diagrams.
documenting security violations
functional job requirements for INFOSEC
 personnel (SA, ISSO, ISSM, DAA, etc.)
best practices in information assurance
hardware, software, firmware
updating operating procedures
maintaining currency of the CONOPS
knowledge of certification tools
legal aspects of testing (limitations to
 monitoring, etc.)
knowledge of operating systems
risk management methodologies
roles and responsibilities of C&A personnel
technical knowledge of networks, servers,
 workstations, operating systems, etc.
understanding of current threats and
 incidents)

UNCLASSIFIED

ANNEX C

REFERENCES AND BIBLIOGRAPHY






The following references pertain to this Instruction:

- a. NSTISSD No. 501, National Training Program for Information Systems Security (INFOSEC) Professionals, November 16, 1992
- b. NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, June 5, 1992
- c. NIST Special Publication No. 800-16, Information Technology Security Requirements: A Role- and Performance-Based Model, April 1998
- d. NSTISSI No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP), April 2000
- e. NCSC-TG-031, Certification and Accreditation Process Handbook for Certifiers
- f. DoD Instruction No. 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP)
- g. I942-TR-002, Version 1, Accreditor's Guideline, July 1994
- h. SC-2610-143-93, Defense Intelligence Management Document, DoD Intelligence Information Systems (DoDIIS) Site Certifier's Guide, November 1993
- i. DoDIIS Systems Security Certification and Accreditation Guide, March 2000 National Information Assurance Partnership (NIAP), URL: <http://niap.nist.gov>
- j. DoD Directive No. 5200.28, Security Requirements for Automated Information Systems March 21, 1988
- k. Public Law No. 100-235, Computer Security Act of 1987, January 8, 1988
- l. NCSC-TG-034, Certification and Accreditation Planning Guide for Program Managers
- m. Office of Management and Budget Circular No. A-130, Management of Federal Information Resources, February 8, 1996
- n. Director of Central Intelligence Directive No. 6/3, Protecting Sensitive Compartmented Information Within Information Systems, June 1999
- o. Common Criteria for Information Technology Security Evaluation (CC) version 2.1, International Standards Organization (ISO) International Standard 15408, January 31, 2000

ANNEX C
NSTISSI No. 4015

G. CNSS Standard NTSTISSI 4016

a. Course Mapping Details

 Print	 Collapse All	 Expand All	 Previous Page	 Next Page
---	--	--	---	---

Welcome Barbara Ciaramitaro, it is Monday, August 16, 2010 at 03:39:36 PM
You are currently viewing a report for CNSSI 4016 sorted by element.

*** = Can include a summary justification for that section.**

▼ FUNCTION 1 - INFORMATION SYSTEM LIFE CYCLE ACTIVITIES

▼ Life Cycle Duties

▼ No Subsection

▼ 2. System Disposition/Reutilization

- ▼ E - Identify agency-specific system reutilization policies and procedures

[HSCJ 202](#)
[MISM 661](#)

- ▼ *E - Discuss processes for disposition of media and data

[HSCJ 202](#)
[MISM 661](#)

▼ 3. System Configuration and Management Board (SCMB)

- ▼ *E - Identify life cycle management SCMB policies and procedures

[HSCJ 202](#)
[MISM 661](#)

▼ 4. Operations & Maintenance (O & M)

- ▼ E - Monitor life cycle operation and maintenance project milestones relating to risk

[HSCJ 202](#)
[MISM 661](#)

- ▼ E - Monitor maintenance procedures concerning life cycle operations and analysis issues

[HSCJ 202](#)
[MISM 661](#)

- ▼ E - Monitor performance measurement data in operations and maintenance examination of events and/or changes in an event

[HSCJ 202](#)
[MISM 661](#)

- ▼ *E - Discuss risk analysis processes used in development of life cycle functions

[HSCJ 202](#)
[MISM 661](#)

▼ 5. System Acquisition

- ▼ E - Monitor process of selecting and purchasing IT designed to implement management risk process

[HSCJ 210](#)
[MISM 661](#)

- ▼ E - Verify that system acquisitions policies and procedures include assessment of risk management policies

[HSCJ 202](#)
[MISM 661](#)

- ▼ *E - Discuss risk analyst concerns relating to life cycle system security planning

HSCJ 202

MISM 661

▼ **6. System Administration**

- ▼*E - Discuss audit mechanism processes used to collect, review, and/or examine system activities

HSCJ 202

MISM 661

▼ **7. System Owners**

- ▼*E - Discuss maintenance plans for protective measures to ensure tolerable level of risk

HSCJ 202

MISM 661

▼ **8. System Developers**

- ▼E - Discuss process to ensure that applications function according to specifications

HSCJ 202

MISM 661

- ▼E - Explain risk methodologies used to evaluate measures taken to protect system

HSCJ 202

MISM 661

- ▼*E - Discuss process for selecting and purchasing new information technology (IT)

HSCJ 202

MISM 661

▼ **9. Computer Science and Architecture**

- ▼*E - Discuss system IA design guidance

HSCJ 202

MISM 661

▼ **10. Security Product Integration**

- ▼E - Examine and analyze applied security

HSCJ 202

MISM 661

▼ **11. Information Systems Security Officer (ISSO) Activities**

- ▼E - Discuss processes for timely deletion of accounts

HSCJ 202

MISM 661

- ▼E - Discuss processes for updating access

HSCJ 202

MISM 661

- ▼E - Discuss processes for verification of authorization prior to adding new account

HSCJ 202

MISM 661

- ▼*E - Discuss maintenance of user accounts

HSCJ 202

MISM 661

▼ **12. Audit Mechanism**

- ▼*E - Review policy, guidance and process for the capture, maintenance, and distribution of audit logs

HSCJ 202

MISM 661

▼13. Policy Development

- ▼E - Develop risk management methodology which includes evaluation of threats, vulnerabilities, and countermeasures

HSCJ 202

MISM 661

▼14. System Certifiers and Accreditors

- ▼E - Explain local policies and procedures to supplement and implement higher-level guidance

HSCJ 202

MISM 661

- ▼*E - Explain how certification process ensures security requirement implementation

HSCJ 202

MISM 661

▼15. Automated Tool for Security Test

- ▼E - Discuss utilities used to determine vulnerabilities or configurations not within established limits/baselines

HSCJ 202

MISM 662

MISM 661

▼FUNCTION 2 - COUNTERMEASURES IDENTIFICATION, IMPLEMENTATION, AND ASSESSMENTS

▼Countermeasures

▼No Subsection

▼1. General

- ▼E - Assist certifier to determine countermeasures based on threat capabilities and motivations

HSCJ 202

MISM 661

- ▼*E - Identify all component and overall risks inherent in system

HSCJ 210

MISM 661

▼2. Analyzing Potential Countermeasures

- ▼E - Assist certifier to evaluate security requirements as potential countermeasures

HSCJ 202

MISM 661

- ▼E - Discuss respective value of penetration testing post-testing actions, general information principles, and summary comparison of network testing techniques

HSCJ 202

MISM 662

MISM 661

- ▼E - Discuss testing roles and responsibilities

HSCJ 202

MISM 661

- ▼ E - Explain process to determine underlying state of system

HSCJ 202

MISM 661

- ▼ E - Relate organization IT security needs to countermeasure requirements

HSCJ 202

MISM 661

- ▼ *E - Discuss security test and evaluation (ST&E) procedures, tools, and equipment

HSCJ 202

MISM 661

▼ 3. Determining Countermeasures

- ▼ E - Apprise decision makers of existing countermeasure models, tools, and techniques

HSCJ 202

MISM 661

▼ 4. Identifying Potential Countermeasures

- ▼ E - Assist certifier/IA engineer to evaluate system security safeguards established to determine system security posture

HSCJ 202

MISM 661

- ▼ E - Discuss effectiveness of automated security tools that verify an individual's eligibility to receive specific categories of information

HSCJ 202

MISM 661

- ▼ E - Discuss methodologies used to evaluate system security safeguards

HSCJ 202

MISM 662

MISM 661

- ▼ *E - Discuss effectiveness of automated security tools that confirm validity of a transmission

HSCJ 202

MISM 661

▼ 5. Determining Cost/Benefit of Countermeasures

- ▼ E - Outline cost/benefit of personnel supporting access control policies

HSCJ 202

MISM 661

- ▼ *E - Outline cost/benefit of organization's IA countermeasure plans

HSCJ 202

MISM 661

▼ FUNCTION 3 - CERTIFICATION AND ACCREDITATION

▼ Certification and Accreditation

▼ No Subsection

▼ 1. Certification and Accreditation Guidelines and Documentation

- ▼ E - Discuss role of RA in certification and accreditation process

HSCJ 202

MISM 661

- ▼*E - Explain applicable organizational certification and accreditation processes
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **2. Vulnerabilities and Attacks**
 - ▼*E - Discuss paired interaction of a vulnerability to an attack
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **4. Security Laws**
 - ▼ E - Outline security laws applicable to certification/accreditation process
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **5. Physical Security Requirements**
 - ▼ E - Discuss risk mitigation decisions derived from analysis and review of physical security requirements
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **6. Security Inspections**
 - ▼ E - Discuss security inspections conducted during C&A process
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼*E - Evaluate security inspections conducted during C&A process
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **7. Security Policies and Procedures**
 - ▼ E - Explain security policies and procedures implemented during risk analysis/assessment process
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **8. Security Processing Mode**
 - ▼ E - Discuss vulnerabilities associated with security processing modes
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **9. System Certification**
 - ▼*E - Discuss threat and vulnerability analyses input to C&A process
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **10. Support C&A**
 - ▼ E - Explain alternative actions permitted on system
 - [HSCJ 202](#)
 - [MISM 661](#)
 - ▼*E - Identify system security policies
 - [HSCJ 202](#)
 - [MISM 661](#)
- ▼ **11. System Security Profile**
 - ▼ E - Assist in helping to identify protections offered by security features in specific configurations

HSCJ 202

MISM 661

- ▼ E - Discuss security features of system

HSCJ 202

MISM 661

- ▼*E - Describe protections offered by security features in specific configurations

HSCJ 202

MISM 661

▼ 12. Threat/Risk Assessment

- ▼*E - Identify threat/risk assessment methodology appropriate for use with system undergoing accreditation

HSCJ 202

MISM 661

▼ 13. Information Technology Security Evaluation Criteria

- ▼ E - Assist in the use of common criteria guidance to determine hardware and software assurance applications for simultaneous processing of a range of information classes

HSCJ 202

MISM 661

▼ 14. Mission

- ▼ E - Discuss impact of security on mission

HSCJ 202

MISM 661

▼ 15. Interviewing/Interrogation

- ▼ E - Assist certifier in preparing questions for determining countermeasures during C&A process

HSCJ 202

MISM 661

▼ 16. Applications Security

- ▼ E - Discuss criticality of applications security

HSCJ 202

MISM 661

▼ FUNCTION 4 - SYNTHESIS OF ANALYSIS

▼ Synthesis of Analysis Duties

▼ A. General

▼ 1. Synthesis of Components and Overall Risks

- ▼ E - Report synthesis of all component and risks inherent in a system

HSCJ 202

MISM 661

▼ 3. Aspects of Security

- ▼ E - Discuss security with regard to confidentiality, integrity, authentication, availability, and non-repudiation

HSCJ 202

MISM 661

▼ 4. Assessment Methodology

- ▼ E - Appraise information acquisition and review process for best use of resources to protect system

HSCJ 202

MISM 661

▼ **5. Associate Threat Probabilities to Vulnerability**

- ▼ E - Describe process of analyzing paired interactions of system threats and vulnerabilities

HSCJ 202

MISM 662

MISM 661

▼ **6. Conducting Risk Analysis**

- ▼ E - Conduct risk analysis examination and evaluation process to determine relationships among threats, vulnerabilities, and countermeasures

HSCJ 202

MISM 661

▼ **7. Countermeasure Analysis**

- ▼ E - Conduct detailed examination and evaluation of possible actions to mitigate vulnerabilities

HSCJ 202

MISM 662

MISM 661

- ▼ *E - Conduct detailed examination and evaluation of impact of attacks

HSCJ 202

MISM 661

▼ **8. Critical Thinking**

- ▼ E - Discriminate between known and hypothetical variables based on executed test procedures

HSCJ 202

MISM 661

▼ **9. Deductive Reasoning**

- ▼ *E - Analyze tests results

HSCJ 202

MISM 661

▼ **10. Detailed Residual Risk**

- ▼ E - Assist certifier/IA engineer in evaluating susceptibility of a system to attack after countermeasures have been applied

HSCJ 202

MISM 661

- ▼ *E - Discuss susceptibility of a system to attack after countermeasures have been applied

HSCJ 202

MISM 662

MISM 661

▼ **13. All Risk Variables**

- ▼ E - Evaluate an analysis of threats, vulnerabilities, attacks, and consequences in relationship to risk assessment of a system

HSCJ 202

MISM 661

▼ **14. Risk Assessment (Environment & Threat Description)**

- ▼ E - Discuss environment in relation to current threat

HSCJ 202

MISM 661

▼ **15. Risk Management Methodology**

- ▼ E - Discuss organizational capability and ability to evaluate threats, and vulnerabilities

HSCJ 202

MISM 661

▼ **16. Security Countermeasures**

- ▼ E - Assist certifier/IA engineer in defining countermeasures directed at specific threats and vulnerabilities

HSCJ 202

MISM 661

▼ **17. Technical Vulnerability**

- ▼ E - Discuss hardware, firmware, communications, or software weaknesses that open an information system to exploitation

HSCJ 202

MISM 662

MISM 661

▼ **18. Threat Analysis**

- ▼ E - Examine methods through which threat agent adversely affects information system, facility, or operation

HSCJ 202

MISM 661

▼ **19. Threat Description**

- ▼ E - Define means through which a threat agent can adversely affect information system, facility, or operation

HSCJ 202

MISM 661

▼ **20. Threat/Risk Assessment**

- ▼ E - Discuss process of formally evaluating degree of threat and describing nature of threat

HSCJ 202

MISM 661

▼ **21. Mission**

- ▼ *E - Discuss information system support mission

HSCJ 202

MISM 661

▼ **22. Vulnerabilities**

- ▼ E - Discuss weakness in an information system, system security procedures, internal controls, or implementation that could be exploited

HSCJ 202

MISM 662

MISM 661

- ▼ E - Explain hardware or software flow that opens an information system to potential exploitation

HSCJ 202

MISM 662

MISM 661

- ▼*E - Assist in identifying weakness in an information system, system security procedures, internal controls, or implementation that could be exploited

HSCJ 202

MISM 662

MISM 661

▼ **23. Vulnerability Analysis**

- ▼*E - Analyze an information system to determine adequacy of security measures

HSCJ 202

MISM 662

MISM 661

▼ **B. Documentation**

▼ **1. Policies**

- ▼E - Discuss agency/local guidance

HSCJ 202

MISM 661

- ▼*E - Explain applicable national level policies

HSCJ 202

MISM 661

▼ **9. Technical Knowledge of Information System**

- ▼E - Outline technical knowledge required of personnel responsible for networks, servers, workstations, operating systems, etc.

HSCJ 202

MISM 661

▼ **C. Effect of Countermeasure**

▼ **9. Security Product Testing/Evaluation**

- ▼E - Examine analysis of security safeguards of a system as they have been applied to an operational environment to determine security posture

HSCJ 202

MISM 662

MISM 661

▼ **10. Technical Knowledge of Information System**

- ▼E - Outline technical knowledge required of personnel responsible for operating and maintaining networks, servers, workstations, operating systems, etc.

HSCJ 202

MISM 661

▼ **FUNCTION 5 - TESTING AND EVALUATION**

▼ **Testing and Evaluation Duties**

▼ **No Subsection**

▼ **3. Account Administration**

- ▼E - Discuss maintenance of accounting files, tools, user accounts, and system statistics

HSCJ 202

MISM 661

▼ **4. Assessment Methodology**

- ▼E - Define vulnerability analysis process

HSCJ 202

MISM 662

MISM 661

▼ **5. Associate Threat Probabilities to Vulnerability**

- ▼ E - Explain paired interaction of system threats and vulnerabilities

HSCJ 202

MISM 662

MISM 661

▼ **6. Audit Trails and Logging**

- ▼ E - Team with certifier/IA engineer to compile chronological record of system activities for reconstruction and examination of events and/or changes in an event

HSCJ 202

MISM 661

▼ **7. Backups**

- ▼ E - Discuss purpose of using copies of backup files for later reconstruction of files

HSCJ 202

MISM 661

▼ **8. Software Test & Evaluation Results**

- ▼ E - Ensure software test and evaluation results related to system restoration are performed

HSCJ 202

MISM 661

▼ **12. Security Test & Evaluation Plan & Procedure**

- ▼ E - Assist with the development of ST&E plan and procedure for testing and evaluating a system

HSCJ 202

MISM 661

▼ **13. Error Logs**

- ▼ E - Interpret files created by operating system for review of audit process

HSCJ 202

MISM 661

▼ **14. Non-Technical & Technical Result**

- ▼ E - Interpret technical and non-technical results from testing and evaluation

HSCJ 202

MISM 661

▼ **15. Evaluation Techniques**

- ▼ E - Team with certifier/IA engineer to integrate technical analysis of components, products, subsystems, or systems security that establishes whether or not component, product subsystem, or system meets a specific set of requirements independently and in

HSCJ 202

MISM 661

▼ **16. Identify All Risk Variables**

- ▼ E - Explain development of a compendium of relative threats, vulnerabilities, attacks, and consequences related to a system (Common vulnerabilities and exploitations)

HSCJ 202

MISM 661

▼ **18. Certification Tools**

- ▼ E - Team with certifier/IA engineer to interpret results of certification tools during testing and evaluation

HSCJ 202

MISM 661

- ▼ **19. Privileges (Class, Nodes)**

- ▼ E - Influence program or user operations that can be performed during testing and Evaluation

HSCJ 202

MISM 661

- ▼ **20. Test and Evaluation Strategies**

- ▼ *E- Identify strengths of alternative test and evaluation strategies

HSCJ 202

MISM 661

- ▼ **21. Testing Implementation of Security Features**

- ▼ E - Integrate testing of security features during testing and evaluation

HSCJ 202

MISM 661

- ▼ **FUNCTION 6 - THREAT AND ADVERSARY ANALYSIS**

- ▼ **Threat and Adversary Analysis Duties**

- ▼ **A. General**

- ▼ **1. Conducting Risk Analysis**

- ▼ E - Conduct examination of vulnerabilities, attack, threats and consequences that may affect system

HSCJ 202

MISM 662

MISM 661

- ▼ **2. Cost/Benefit Analysis**

- ▼ E - Conduct an assessment of costs of data protection for a system versus cost of loss or compromise

HSCJ 202

MISM 661

- ▼ **3. Critical Thinking**

- ▼ E - Discuss known and hypothetical variables based on test procedures

HSCJ 202

MISM 661

- ▼ **4. Deductive Reasoning**

- ▼ E - Recommend solutions based on a set of static and variable factors of system

HSCJ 202

MISM 661

- ▼ **5. Effects of Mitigation**

- ▼ E - Determine effects of mitigation derived from application of countermeasures to a system

HSCJ 202

MISM 661

- ▼ **6. Hostile Intelligence Sources**

- ▼ E - Discuss impact of hostile agents seeking national security information which could potentially cause harm to national security

HSCJ 202

ISIN 330

MISM 661

▼ **7. All Risk Variables**

- ▼ E - Build a compendium of relative threats, vulnerabilities, attacks, and consequences related to system

HSCJ 202

MISM 661

▼ **B. Risk Assessment (Environment & Threat Description)**

▼ **1. Risk Management Methodology**

- ▼ E - Discuss evaluation of threats, vulnerabilities, and countermeasures to determine residual risk

HSCJ 202

MISM 661

▼ **2. Security Countermeasures**

- ▼ E - Discuss security and software countermeasures during design, implementation, and testing phases to achieve required level of confidence

HSCJ 202

MISM 661

▼ **3. Threat Analysis**

- ▼ E - Conduct examination and evaluation of sources and factors that can adversely impact system

HSCJ 202

MISM 662

MISM 661

▼ **4. Treat Description**

- ▼ E - Identify level of threat based on its applicability to system

HSCJ 202

MISM 661

▼ **5. Threat/Risk Assessment**

- ▼ E - Recommend life cycle countermeasures based on assessments of threats, capabilities, and motivations to exploit vulnerability

HSCJ 202

MISM 661

▼ **6. Mission**

- ▼ E - Determine if an adverse system finding should be allowed to halt mission support operations

HSCJ 202

MISM 661

- ▼ *E - Discuss current mission and role of information system in supporting mission

HSCJ 202

MISM 661

▼ **7. Vulnerability Analysis**

- ▼ E - Appraise weaknesses in information system, security procedures, internal controls, or implementations that could be exploited

HSCJ 202

MISM 662

MISM 661

▼ **D. Agency-Specific Policies and Procedures**

▼ **1. Agency-Specific Policies and Procedures**

- ▼ E - Discuss local policies and procedures implementing regulations, laws, and procedures in local environment

HSCJ 202

MISM 661

▼ **H. Technical Surveillance Countermeasures**

▼ **1. Technical Surveillance Countermeasures**

- ▼ E - Discuss Techniques and measures to detect and neutralize a wide variety of hostile penetration technologies

HSCJ 202

MISM 662

MISM 661

▼ **FUNCTION 7 - MISSION AND ASSETS ASSESSMENTS**

▼ **Mission and Assets Duties**

▼ **A. General**

▼ **1. Conducting Risk Analysis**

- ▼ E - Conduct detailed examination of vulnerabilities, attack, threats, and consequences that may affect system

HSCJ 202

MISM 661

- ▼ *E - Conduct detailed evaluation of vulnerabilities, attack, threats, and consequences that may affect system

HSCJ 202

MISM 661

▼ **2. Cost/Benefit Analysis**

- ▼ E - Conduct cost assessment for providing data protection versus cost of data loss or compromise

HSCJ 202

MISM 661

▼ **3. Critical Thinking**

- ▼ E - Understand known and hypothetical variables based on test procedures

HSCJ 202

MISM 661

▼ **4. Deductive Reasoning**

- ▼ E - Recommend solutions based on a set of static and variable factors

HSCJ 202

MISM 661

▼ **5. Effects of Mitigation**

- ▼ E - Determine effects of mitigation derived from application of countermeasures

HSCJ 202

MISM 661

▼ **6. Hostile Intelligence Sources**

- ▼ E - Discuss impact of hostile agents seeking national security information which could potentially cause harm to national security

HSCJ 202

ISIN 330

MISM 661

▼ **7. All Risk Variables**

- ▼ E - Build a compendium of relative threats, vulnerabilities, attacks, and consequences related to system

HSCJ 202

MISM 661

▼ **B. Risk Assessment (Environment & Threat Description)**

▼ **1. Risk Management Methodology**

- ▼ E - Discuss evaluation of threats, vulnerabilities, and countermeasures to determine residual risk

HSCJ 202

MISM 661

▼ **2. Security Countermeasures**

- ▼ E - Discuss security and software countermeasures during design, implementation and testing phases to achieve required level of confidence

HSCJ 202

MISM 661

▼ **3. Threat Analysis**

- ▼ *E - Conduct detailed examination and evaluation of sources and factors that can adversely impact system

HSCJ 202

MISM 661

▼ **4. Treat Description**

- ▼ E - Identify level of threat based on its applicability to system

HSCJ 202

MISM 661

▼ **5. Threat/Risk Assessment**

- ▼ E - Recommend life cycle countermeasures based on assessment of threats, capabilities, and motivations to exploit vulnerability

HSCJ 202

MISM 661

▼ **6. Mission**

- ▼ E - Assess mission to determine if an adverse finding should be allowed to affect continued IT operations in a given mission environment

HSCJ 202

MISM 661

▼ **7. Vulnerability Analysis**

- ▼ E - Appraise exploitable weaknesses in information system, security procedures, internal controls or implementations

HSCJ 202

MISM 662

MISM 661

▼ **D. Agency-Specific Policies and Procedures**

▼ **1. Agency-Specific Policies and Procedures**

- ▼ E - Discuss local policies and procedures implementing regulations, laws, and procedures in local environment

HSCJ 202

MISM 661

▼ **H. Technical Surveillance Countermeasures**

▼ **1. Technical Surveillance Countermeasures**

- ▼ E - Discuss techniques and measures to detect and neutralize hostile penetration technologies

HSCJ 202

MISM 662

MISM 661

▼ **FUNCTION 8 - VULNERABILITIES AND ATTACK AVENUES ANALYSIS**

▼ **Vulnerability and Attack Avenues Duties**

▼ **A. General**

▼ **1. Vulnerabilities, attacks, threats, and consequences**

- ▼ E - Assess vulnerabilities, attacks, threats, and consequences to determine vulnerabilities and attack avenues

HSCJ 202

MISM 662

MISM 661

▼ **2. Cost/Benefit Analysis**

- ▼ E - Discuss cost analysis of data protection versus cost of data lose or compromise

HSCJ 202

MISM 661

▼ **3. Critical Thinking**

- ▼ E - Apply discrimination to known and potential vulnerabilities based on test procedures

HSCJ 202

MISM 662

MISM 661

▼ **4. Deductive Reasoning**

- ▼ E - Use test results to determine underlying state of system

HSCJ 202

MISM 661

▼ **5. Effect of Countermeasures on Risk**

- ▼ E - Determine effect of countermeasures on risk through the analysis of paired interaction of a defense

HSCJ 202

MISM 661

▼ **6. Effects of Mitigation**

- ▼ E - Determine effects of mitigation derived from application of countermeasures to system

HSCJ 202

MISM 661

▼ **7. Hostile Intelligence Sources**

- ▼ E - Discuss hostile intelligence sources as part of vulnerabilities and attack venues

HSCJ 202

ISIN 330

MISM 661

▼ **8. Risk Variables**

- ▼ E - Identify risk variables to build a compendium of relative threats, vulnerabilities, attacks, and consequences related to a system

HSCJ 202

MISM 661

▼ **9. Jamming**

- ▼ E - Discuss jamming as a potential threat

HSCJ 202

MISM 661

▼ **10. Risk Assessment**

- ▼ E - Define risk assessment methodology in relation to risk analyst function

HSCJ 202

MISM 661

▼ **11. Risk Management Methodology**

- ▼ E - Define risk management methodology in relation to system security

HSCJ 202

MISM 661

▼ **12. Security Countermeasures**

- ▼ E - Discuss security countermeasures in relation to vulnerabilities and attack venues

HSCJ 202

MISM 661

▼ **13. Threat Analysis**

- ▼ E - Use threat analysis to determine vulnerabilities and attack venues

HSCJ 202

MISM 661

▼ **14. Threat/Risk Assessment**

- ▼ E - Apply threat and/or risk assessment in determining vulnerabilities and attack venues

HSCJ 202

MISM 661

▼ **15. Mission**

- ▼ E - Support organizational mission in conjunction with vulnerabilities and attack venues

HSCJ 202

MISM 661

▼ **16. Vulnerabilities**

- ▼ E - Discuss weaknesses in system, system security procedures, and internal controls and implementation

HSCJ 202

MISM 662

MISM 661

▼ **17. Vulnerability Analysis**

- ▼ E - Use vulnerability analysis to determine adequacy of security measures, identify security deficiencies, and provide data to predict effectiveness of security measures

HSCJ 202
MISM 662
MISM 661

▼ **B. Developing Attack Avenues**

▼ **1. Avenues of Attack**

- ▼ E - Describe known avenues of attack such as operating system bugs, network vulnerabilities, human threats, etc.

HSCJ 202
MISM 661

▼ **C. Characterizing Vulnerabilities**

▼ **1. Characterizing Vulnerabilities**

- ▼ E - Evaluate threats and vulnerabilities

HSCJ 202
MISM 662
MISM 661

- ▼ *E - Discuss aspects of security in a vulnerability testing and evaluation plan

HSCJ 202
MISM 661

▼ **D. Researching Vulnerability Report**

▼ **1. Researching Vulnerability Report**

- ▼ E - Evaluate vulnerability assessment methodologies

HSCJ 202
MISM 662

▼ **E. Collecting and Reviewing Vulnerabilities**

▼ **1. Collecting and Reviewing Vulnerabilities**

- ▼ *E - List potential vulnerabilities that may lead to defeat of security services

HSCJ 202
MISM 662
MISM 661

▼ **F. Comparing and Contrasting Attack Avenues**

▼ **1. Comparing and Contrasting Attack Avenues**

- ▼ E - Evaluate payoff to and liabilities incurred by an attacker in a successful attack

HSCJ 202
MISM 662
MISM 661

- ▼ *E - Discuss techniques and measures to detect or neutralize a wide variety of hostile penetration technologies

HSCJ 202
MISM 662
MISM 661

▼ **G. Risk of Detection and Response**

▼ **1. Risk of Detection and Response**

- ▼ E - Characterize impact of security breaches and estimate an attacker's probable Response

HSCJ 202
MISM 661

▼ **I. Technology Necessary to Mount Attack**

▼ **1. Technology Necessary to Mount Attack**

- ▼ E - Describe technology needed to mount an attack based on existing countermeasures

HSCJ 202
MISM 662
MISM 661

▼ **FUNCTION 9 - TRAINING AND AWARENESS**

▼ **Training and Awareness Duties**

▼ **A. Policies/Procedures/Methodology**

▼ **1. Access Control Policies**

- ▼ *E - Summarize national and local level access control policies

HSCJ 202
MISM 661

▼ **2. Laws, Regulations, and Other Public Policy**

- ▼ E - Discuss applicable IA laws, regulations, and policies

HSCJ 202
MISM 661

- ▼ *E - Identify local application of IA laws, regulations, and policies

HSCJ 202
MISM 661

▼ **3. Agency-Specific IA and IT Policies and Procedures**

- ▼ *E - Summarize agency-specific policies and procedures in relation to risk environment

HSCJ 202
MISM 661

▼ **5. Audit Trails and Logging Policies**

- ▼ *E - Discuss audit trails and logging policies

HSCJ 202
MISM 661

▼ **6. Change Control Policies**

- ▼ *E - Discuss change control policies for incorporation in IA training

HSCJ 202
MISM 661

▼ **7. Communications Security Policy and Guidance**

- ▼ E - Identify communications security policy and guidance for incorporation into IT training

HSCJ 202
MISM 661

- ▼ *E - Discuss communications security policy and guidance for incorporation into IT training

HSCJ 202
MISM 661

▼ **8. Emergency Destruction Planning and Procedures (EDPP)**

- ▼ *E - Discuss EDPP for incorporation in IA training

HSCJ 202

MISM 661

▼ **9. Personnel Security Policies and Guidance**

- ▼ E - Discuss role of personnel security policies and guidance as part of overall risk management plan

HSCJ 202

MISM 661

▼ **10. Formal Methods for Security Design**

- ▼ E - Outline role of formal methods in security design as part of risk management plan

HSCJ 202

MISM 661

▼ **11. Information Categorization**

- ▼ E - Discuss various categorization schemas

HSCJ 202

MISM 661

▼ **12. Information Classification**

- ▼ *E - Discuss classification policies as part of risk management plan

HSCJ 202

MISM 661

▼ **14. Methods of Defining Security Requirements**

- ▼ *E - Discuss definitions of security requirements

HSCJ 202

MISM 661

▼ **15. Physical Security Requirements**

- ▼ *E - Discuss physical security requirements

HSCJ 202

MISM 661

▼ **17. Risk Management Methodology**

- ▼ E - Summarize approaches to risk management

HSCJ 202

MISM 661

▼ **B. Technology**

▼ **1. Applications Security**

- ▼ E - Discuss state of security features embedded in commercial-off-the-shelf (COTS) products in relation to risk management plan

HSCJ 202

MISM 661

▼ **2. Database Security Features**

- ▼ E - Identify critical database security pitfalls

HSCJ 202

MISM 610

- ▼ E - List database best practices and pitfalls in database security

HSCJ 202

MISM 610

- ▼ *E - Discuss elements of database security features

HSCJ 202

MISM 610

▼ **3. Distributed Systems Security**

- ▼ E - Discuss risks associated with distributed systems security

HSCJ 202

MISM 661

▼ **4. Firmware Security**

- ▼ E - Discuss differences between security features and capabilities

HSCJ 202

MISM 661

▼ **7. Network Security Software**

- ▼ E - Discuss state and vulnerabilities in network security software

HSCJ 202

MISM 662

MISM 670

▼ **9. Technology Trends**

- ▼ E - Summarize technology trends in context of future security management plan

HSCJ 202

MISM 661

▼ **10. Environmental/Natural Threats**

- ▼ E - Discuss environmental and natural threats as part of security management plan

HSCJ 202

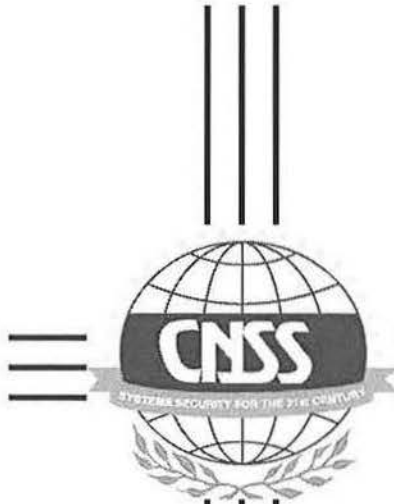
MISM 661

- ▼ *E - List environmental and natural threats as part of security management plan

HSCJ 202

MISM 661

b. Standard Specifications



National Information Assurance Training Standard For Risk Analysts

Awareness, Training and Education (AT&E) are cost-effective methods of improving organizational Information Assurance (IA). In times of ever-contracting budgets, it is difficult to persuade management to spend money on security and training activities that have no direct impact on the organizational bottom line. This paper describes the proficiencies used to aid in the systematic development of training to serve as the first line of defense in Information Assurance (IA). In addition it describes how these materials are applicable to your organizational long-range plans.

This document provides minimum training standards for those performing risk analyst functions for national security systems. It also may offer guidelines for those performing risk analyst functions for unclassified systems. Your department or agency may require a more stringent implementation.

COMMITTEE ON NATIONAL SECURITY SYSTEMS

CNSSI No. 4016

NATIONAL MANAGER**FOREWORD**

1. Since the September 11th terrorist attacks against the sovereignty of the United States and its people, both the President and the Congress have redoubled their efforts to underpin the nation's security. The following guidance, reflecting their support, is intended to assist all federal agencies and private sector concerns in protecting their information systems (ISs). Only through diligence and a well-trained workforce will we be able to defend adequately the nation's vital information resources.

2. This instruction establishes the minimum training standard for the development and implementation of Information Assurance (IA) training for Risk Analysts (RA). The standard presents an in-depth analysis of the range of skills required for persons performing RA functions. RA-related responsibilities may be found throughout government and industry under the guise of other occupational headings such as data analyst, budget analyst, and even to some degree, chief information officer. This standard, while codifying the core performance requirements for a dedicated RA, also provides a set of performance measures which can be incorporated into the definition of positions with RA-related responsibilities in the IA, IT, and management areas.

3. Additional copies of this instruction can be obtained on the CNSS website at www.cnss.gov or by contacting the CNSS Secretariat at the address below.

/s/

KEITH B. ALEXANDER
Lieutenant General, U.S. Army

RISK ANALYST

NATIONAL INFORMATION ASSURANCE (IA) TRAINING STANDARD FOR RISK ANALYSTS

	<u>SECTION</u>
PURPOSE	I
REFERENCES	II
DEFINITIONS.....	III
APPLICABILITY.....	IV
RESPONSIBILITIES	V

SECTION I – PURPOSE

1. This instruction establishes the minimum training standard for the development and implementation of Information Assurance (IA) training for Risk Analysts (RA).

SECTION II – REFERENCES

2. Referenced documents are listed in ANNEX B.

SECTION III – DEFINITIONS

3. Definitions in CNSS Instruction No. 4009 (Reference a) and National Security Telecommunications and Information Systems Security Directive (NSTISSD) No. 501 (Reference b) apply to this instruction.

SECTION IV – APPLICABILITY

4. The President’s National Strategy to Secure Cyberspace (Reference c), NSTISSD No. 501, and the Federal Information Security Management Act (FISMA) (Reference d), establish the requirements for federal departments and agencies to implement training programs for IA professionals. An IA professional is an individual responsible for the security oversight or management of national security systems during phases of the life cycle. These issuances and others are being implemented in a synergistic environment among departments and agencies committed to satisfying IA education and training requirements. This instruction is a continuation in a series of minimum training and education standards being developed to assist departments and agencies in meeting their responsibilities. (References e through i).

5. ANNEX A lists the minimal IA performance standard for an RA. The body of knowledge listed in this instruction was obtained collaboratively from a variety of sources, *i.e.*, the CNSS Community, industry, and academia.

6. This instruction is applicable to all departments and agencies of the U.S. Government and their contractors responsible for the development and implementation of IA training for RAs and RA-related positions.

7. Nothing in this policy alters or supersedes the existing authorities of the Director of National Intelligence.

SECTION V – RESPONSIBILITIES

8. Heads of U.S. Government departments and agencies shall ensure that RAs (or their equivalents) are trained to the level of proficiency outlined in this instruction, and that such training is provided to those requiring it at the earliest practicable date.

9. The National Manager shall:

- a. Maintain and provide an IA training standard for RAs to U.S. Government departments and agencies.
- b. Ensure that appropriate IA training courses for RAs are developed.
- c. Assist other U.S. Government departments and agencies in developing and/or conducting IA training activities for RAs as requested.
- d. Maintain a national clearinghouse for training and education materials.

Encls:

ANNEX A - Minimal IA Performance Standard for RA

ANNEX B - References

ANNEX A

MINIMAL INFORMATION ASSURANCE (IA) PERFORMANCE STANDARD FOR RISK ANALYSTS (RA)

<u>Description</u>	<u>Page</u>
Functions	A-1
Terminal Objective	A-2
General Background	A-4
Function Performance Requirements	
One – Information Life Cycle Activities	A-5
Two – Countermeasures, Identification, Implementation, and Assessments	A-8
Three – Certification and Accreditation	A-10
Four – Synthesis of Analysis	A-12
Five – Testing and Evaluation	A-18
Six – Threat and Adversary Analysis	A-20
Seven – Mission and Assets Management	A-23
Eight – Vulnerabilities and Attack Avenues Analysis	A-26
Nine – Training and Awareness	A-29

FUNCTIONS:

The IA functions performed by personnel engaged in RA activities are:

1. **Information System Life Cycle Activities:** The RA assists other IA professionals in assessing and mitigating risks during the design, development, implementation, operation, maintenance, and disposition phases of information systems life cycle.
2. **Countermeasures Identification, Implementation, and Assessments:** The RA provides a synthesis of risk and countermeasures effectiveness information.
3. **Certification and Accreditation:** The RA provides a repeatable process to assess information system security threats, vulnerabilities and assets and provides risk information to the organization's decision makers.
4. **Synthesis of Analysis:** The RA creates a relevant, sufficient, and comprehensible synthesis of paired-threat/vulnerability, countermeasure, and mission impact information in a context to support decision makers.

5. **Testing and Evaluation:** The RA assesses potential sources of threat that may adversely impact an information system and its associated resources in terms of mission objectives and jeopardy tolerance.

6. **Threat and Adversary Analysis:** The RA assesses potential threats to information systems in terms of mission adversaries, their access to a system, their motivation, and their ability to effect harm.

7. **Mission and Assets Assessments:** The RA assesses how an information system supports a given mission and how a given information system's degradation impacts that mission.

8. **Vulnerabilities and Attack Avenues Analysis:** The RA identifies and characterizes the information system's weaknesses with respect to their cost (resource/jeopardy to themselves) to exploit, an attacker's objectives, access requirements, jeopardy incurred, and the impact on an organization's mission.

9. **Training and Awareness:** The RA serves as a subject matter expert on risk analysis by providing training and informational material to an organization. This material enables trainers to include risk management in courseware and system orientation.

TERMINAL OBJECTIVE:

At the end of training, each skill level will be able to fulfill the following roles:

ENTRY LEVEL: Given various scenarios and typical situations containing information system security issues, the RA under the purview of a more experienced risk analyst will be able to serve as a risk analysis team member, gather information pertinent to IA risk analysis, and provide guidance to IA personnel, *i.e.* system administrators (SAs) and information systems security officers (ISSOs). To be acceptable, the description and application must be in accordance with applicable IA regulations, policies, and guidelines.

INTERMEDIATE LEVEL: Given various scenarios and typical situations containing information system security issues, the RA under the purview of a more experienced risk analyst will be able to interpret and analyze input; explain and recommend appropriate technical, policy, and personnel solutions to system security deficiencies; and to play a leading role in evaluation teams that assess risk. To be acceptable, the description and application must be in accordance with applicable IA regulations, policies, and guidelines.

ADVANCED LEVEL: Given various scenarios and typical situations containing information system security issues, the RA will be able to validate solutions and to verify that the appropriate technical, policy, and personnel remedies to system security deficiencies have been addressed appropriately. The RA also will be able to create new solutions to unexpected problems and to interact with and explain cost/benefit to organizational management. Risk Analysts at the advanced level additionally will be able to mentor and to provide technical guidance to less experienced RAs. To be acceptable, the description and application must be in accordance with applicable IA regulations, policies, and guidelines.

These skill levels* are annotated in the list of performance items under competencies as:

E = Entry Level

I = Intermediate Level

A = Advanced Level

*Note: These levels are linearly hierarchical.

GENERAL BACKGROUND

The following items constitute examples of basic literacies necessary for a Risk Analyst to proceed through the course material based on this standard.

Literacy Necessary for a Risk Analyst at the Entry and Intermediate Level	
Access authorization/permission	Hackers and unauthorized users
Accountability	Information Assurance
Assurance	Information integrity
Audit collection	Intrusion
Automated security tools	Integrity
Business recovery	Life cycle system security
Certification & Accreditation	Penetration testing
Change control policies	Personnel security policies
Classification policies	Physical security
Computer crime	Risk analysis
Configuration management	Risk analysis processes
Continuity of operations	Risk management
Cost benefit analysis	Security laws and regulations
Critical assets	Security policy
Data access control	Security safeguards
Denial of service	Security test and evaluation (ST&E) procedures
Detection and response	Social Engineering
Due diligence	System protection profile
Effect of countermeasures	Threat/vulnerability analyses
Environmental/natural threats	Unauthorized system access
Evidence collections	Vulnerability analysis tools
FISMA	

In each of the competency areas listed below, the RA shall be trained to perform the following functions at the levels indicated:

FUNCTION ONE – INFORMATION SYSTEM LIFE CYCLE ACTIVITIES

Assessing risk throughout system life cycle.

Life Cycle Duties

1. Agency/Vendor Cooperation/Coordination
 - I – Analyze roles and responsibilities of agency vendors as members of risk management team
 - I – Identify roles and responsibilities of agency vendors as member of risk management team
 - A – Recommend changes to roles and responsibilities of agency vendors as member of risk management team

2. System Disposition/Reutilization
 - E – Discuss processes for disposition of media and data
 - E – Identify agency-specific system reutilization policies and procedures
 - I – Examine disposition of media and data records
 - A – Analyze disposition and reutilization records for potential vulnerabilities

3. System Configuration and Management Board (SCMB)
 - E – Identify life cycle management SCMB policies and procedures
 - I – Advise SCMB on risk associated with agency-specific policies and procedures
 - I – Apply risk management methodologies to study of life cycle management policies and procedures
 - I – Assess the risk of change proposals to authorized baselines
 - A – Recommend risk management methodology changes to life cycle management policies and procedures plan

4. Operations & Maintenance (O & M)
 - E – Discuss risk analysis processes used in development of life cycle functions
 - E – Monitor life cycle operation and maintenance project milestones relating to risk
 - E – Monitor maintenance procedures concerning life cycle operations and analysis issues
 - E – Monitor performance measurement data in operations and maintenance examination of events and/or changes in an event
 - I – Consult records of system activities for chronological, analytical reconstruction,

ANNEX A to
CNSSI No. 4016

and maintenance of IA components in IT systems

5. System Acquisition

E – Discuss risk analyst concerns relating to life cycle system security planning

E – Monitor process of selecting and purchasing IT designed to implement management risk process

E – Verify that system acquisitions policies and procedures include assessment of risk management policies

I – Influence process of selecting and purchasing new IT

6. System Administration

E – Discuss audit mechanism processes used to collect, review, and/or examine system activities

I – Recommend software options that control hardware and other software functions

I – Define access permission granted to a subject in relation to an object

I – Define maintenance of user authentication data used to authenticate an identity or to authorize access to data

I – Discuss security software designed to detect and prevent unauthorized system access

7. System Owners

E – Discuss maintenance plans for protective measures to ensure tolerable level of risk

I – Recommend risk management methodologies to evaluate threats, vulnerabilities, and countermeasures to determine residual risk

I – Define legal process for obtaining/maintaining ownership of information

8. System Developers

E – Discuss process for selecting and purchasing new information technology (IT)

E – Discuss process to ensure that applications function according to specifications

E – Explain risk methodologies used to evaluate measures taken to protect system

I – Analyze maintenance practices, procedures, and measures intended to ensure an acceptable level of risk

I - Explain system IA policy with regard to the acquisition and upgrade of software and hardware components and the laws and procedures that must be observed in their implementation

9. Computer Science and Architecture

E – Discuss system IA design guidance

I – Explain collection of verification and validation tools and techniques

I – Explain development of agency-specific IA principles and practices

10. Security Product Integration

E – Examine and analyze applied security

11. Information Systems Security Officer (ISSO) Activities

- E – Discuss maintenance of user accounts
- E – Discuss processes for timely deletion of accounts
- E – Discuss processes for updating access
- E – Discuss processes for verification of authorization prior to adding new account
- I - Explain system IA policy with regard to the acquisition and upgrade of software and hardware components and the laws and procedures that must be observed in their implementation
- I – Discuss maintenance of accounting files, tools, user accounts, and system statistics
- I – Explain process used to collect, review, and/or examine system activities

12. Audit Mechanism

- E – Review policy, guidance and process for the capture, maintenance, and distribution of audit logs
- I – Discuss policies regarding audit data usage, management, and maintenance
- I – Discuss policies regarding personnel access to audit records
- I – Interpret guidance defining audit collection requirements implementation

13. Policy Development

- E – Develop risk management methodology which includes evaluation of threats, vulnerabilities, and countermeasures

14. System Certifiers and Accreditors

- E – Explain how certification process ensures security requirement implementation
- E – Explain local policies and procedures to supplement and implement higher-level guidance
- I – Evaluate operating and management procedures designed to detect or prevent unauthorized access
- I – Evaluate operating and management procedures enforcing access control

15. Automated Tool for Security Test

- E – Discuss utilities used to determine vulnerabilities or configurations not within established limits/baselines

FUNCTION TWO - COUNTERMEASURES IDENTIFICATION, IMPLEMENTATION, AND ASSESSMENTS

Analyzing countermeasure effectiveness to maximize risk mitigation.

Countermeasures

1. General

- E – Identify all component and overall risks inherent in system
- E – Assist certifier to determine countermeasures based on threat capabilities and motivations
- I – Compare examination and evaluation of potential alternative actions to mitigate risk
- I – Determine effects of risk mitigation derived from system countermeasures
- I – Identify risk variables through compendium of threats, vulnerabilities, attacks and consequences
- I – Recommend specific security and software engineering applications during design, implementation, and testing phases
- A – Analyze paired interaction of defense for specific vulnerability related to probability of attack

2. Analyzing Potential Countermeasures

- E – Discuss security test and evaluation (ST&E) procedures, tools, and equipment
- E – Assist certifier to evaluate security requirements as potential countermeasures
- E – Relate organization IT security needs to countermeasure requirements
- E – Discuss testing roles and responsibilities
- E – Discuss respective value of penetration testing post-testing actions, general information principles, and summary comparison of network testing techniques
- E – Explain process to determine underlying state of system
- I – Apply deductive reasoning to test results
- I – Apply discriminate approach variables and constants based on test procedures to gain acceptance for joint system usage
- I – Assist certifier to determine underlying state of system
- A – Analyze potential applicability of network and vulnerability scanning tools
- A – Analyze potential applicability of range of testing tools
- A – Appraise applicability of network tools, *viz.*, password cracking, log review, file integrity, virus detectors, war dialing, wireless LAN testing (war driving), *etc.* software

3. Determining Countermeasures

- E – Apprise decision makers of existing countermeasure models, tools, and techniques

4. Identifying Potential Countermeasures

E – Discuss effectiveness of automated security tools that confirm validity of a transmission

E – Discuss effectiveness of automated security tools that verify an individual's eligibility to receive specific categories of information

E – Discuss methodologies used to evaluate system security safeguards

E – Assist certifier/IA engineer to evaluate system security safeguards established to determine system security posture

I – Research protection profiles for proposed system security countermeasures for a given attack analysis

5. Determining Cost/Benefit of Countermeasures

E – Outline cost/benefit of organization's IA countermeasure plans

E – Outline cost/benefit of personnel supporting access control policies

I – Define cost/benefits of IA plans to determine totality of sensitivity during development, procurement, and installation of system in terms of aggregation of risk

A – Appraise cost/benefit of standard certification tools to support countermeasure activities

FUNCTION THREE – CERTIFICATION AND ACCREDITATION

Verifying validity of and analyzing results of certification and accreditation (C&A) efforts.

Certification and Accreditation

1. Certification and Accreditation Guidelines and Documentation
 - E – Explain applicable organizational certification and accreditation processes
 - E – Discuss role of RA in certification and accreditation process
 - I – Contrast organizational certification and accreditation process with other agency certification and accreditation guidelines
2. Vulnerabilities and Attacks
 - E – Discuss paired interaction of a vulnerability to an attack
 - I – Monitor certification/accreditation process for vulnerabilities
3. Approval to Operate
 - I – Discuss approval process for operating system at a satisfactory level of risk
4. Security Laws
 - E – Outline security laws applicable to certification/accreditation process
5. Physical Security Requirements
 - E – Discuss risk mitigation decisions derived from analysis and review of physical security requirements
6. Security Inspections
 - E – Evaluate security inspections conducted during C&A process
 - E – Discuss security inspections conducted during C&A process
 - I – Recommend security inspections during C&A process
7. Security Policies and Procedures
 - E – Explain security policies and procedures implemented during risk analysis/assessment process
8. Security Processing Mode
 - E – Discuss vulnerabilities associated with security processing modes
9. System Certification
 - E – Discuss threat and vulnerability analyses input to C&A process
 - I – Define activities that support C&A process

- I – Define how C&A provides assurance that controls are functioning effectively
10. Support C&A
 - E – Identify system security policies
 - E – Explain alternative actions permitted on system
 - I – Advise on types and details of actions permitted on systems
 - I – Assist certifier in analyzing, recommending and detailing alternative actions permitted on system
 11. System Security Profile
 - E – Describe protections offered by security features in specific configurations
 - E – Discuss security features of system
 - E – Assist in helping to identify protections offered by security features in specific configurations
 - I – Provide input for recommending security features in specific configurations
 12. Threat/Risk Assessment
 - E – Identify threat/risk assessment methodology appropriate for use with system undergoing accreditation
 - A – Perform threat/risk assessment in support of C&A process
 13. Information Technology Security Evaluation Criteria
 - E – Assist in the use of common criteria guidance to determine hardware and software assurance applications for simultaneous processing of a range of information classes
 14. Mission
 - E – Discuss impact of security on mission
 15. Interviewing/Interrogation
 - E – Assist certifier in preparing questions for determining countermeasures during C&A process
 16. Applications Security
 - E – Discuss criticality of applications security

FUNCTION FOUR – SYNTHESIS OF ANALYSIS

Synthesizing the results of IA efforts taken to protect the system and the data processed on it.

Synthesis of Analysis Duties

A. General

1. Synthesis of Components and Overall Risks
E – Report synthesis of all component and risks inherent in a system
2. Analyze Vulnerabilities and Attacks
I – Compare analysis of paired interaction of vulnerability to attack
3. Aspects of Security
E – Discuss security with regard to confidentiality, integrity, authentication, availability, and non-repudiation
4. Assessment Methodology
E – Appraise information acquisition and review process for best use of resources to protect system
5. Associate Threat Probabilities to Vulnerability
E – Describe process of analyzing paired interactions of system threats and vulnerabilities
6. Conducting Risk Analysis
E – Conduct risk analysis examination and evaluation process to determine relationships among threats, vulnerabilities, and countermeasures
7. Countermeasure Analysis
E – Conduct detailed examination and evaluation of impact of attacks
E – Conduct detailed examination and evaluation of possible actions to mitigate vulnerabilities
8. Critical Thinking
E – Discriminate between known and hypothetical variables based on executed test procedures
9. Deductive Reasoning
E – Analyze tests results

I – Determine underlying state of system

10. Detailed Residual Risk
E – Discuss susceptibility of a system to attack after countermeasures have been applied
E – Assist certifier/IA engineer in evaluating susceptibility of a system to attack after countermeasures have been applied
11. Effect of Countermeasures on Risk
I – Conduct analysis of countermeasure effectiveness as applied to a given risk and probability of an occurrence
12. Effects of Mitigation
I – Determine effects of mitigation derived from application of countermeasures
13. All Risk Variables
E – Evaluate an analysis of threats, vulnerabilities, attacks, and consequences in relationship to risk assessment of a system
14. Risk Assessment (Environment & Threat Description)
E – Discuss environment in relation to current threat
15. Risk Management Methodology
E – Discuss organizational capability and ability to evaluate threats, and vulnerabilities
16. Security Countermeasures
E – Assist certifier/IA engineer in defining countermeasures directed at specific threats and vulnerabilities
17. Technical Vulnerability
E – Discuss hardware, firmware, communications, or software weaknesses that open an information system to exploitation
18. Threat Analysis
E – Examine methods through which threat agent adversely affects information system, facility, or operation
19. Threat Description
E – Define means through which a threat agent can adversely affect information system, facility, or operation
20. Threat/Risk Assessment

E – Discuss process of formally evaluating degree of threat and describing nature of threat

21. Mission

E – Discuss information system support mission

I – Determine offsets of adverse findings and decision to continue IT operation in current mission environment

22. Vulnerabilities

E – Assist in identifying weakness in an information system, system security procedures, internal controls, or implementation that could be exploited

E – Discuss weakness in an information system, system security procedures, internal controls, or implementation that could be exploited

E – Explain hardware or software flow that opens an information system to potential exploitation

23. Vulnerability Analysis

E – Analyze an information system to determine adequacy of security measures

I – Analyze weakness in an information system, system security procedures, internal controls, or implementation that could be exploited

I – Identify security deficiencies

I – Assist certifier/IA engineer provide data that confirms effectiveness of security measures after security testing

I – Assist certifier/IA engineer to provide data to predict effectiveness of a security measure testing

B. Documentation

1. Policies

I – Identify applicable national level and agency/local policies and guidance

E – Explain applicable national level policies

E – Discuss agency/local guidance

2. Access Control Policies

I - Explain system IA policy with regard to the acquisition and upgrade of software and hardware components and the laws and procedures that must be observed in their implementation

3. Formal Methods for Security Design

I – Team with certifier/IA engineer to evaluate collection of languages and tools that enforce methods of verification

4. Generally Accepted Systems Security Principles

I – Team with certifier/IA engineer to evaluate acceptability of using federal information security practices in system design and protection

A – Team with certifier/IA engineer to plan and coordinate development of IA principles and practices applied to coordination with OMB and with technical assistance from NSA

5. Information Security Policy

I – Evaluate security policies that describe permitted actions that may have an adverse affect on system

6. Laws, Regulations, and Other Public Policy

I – Evaluate the implementation of laws, regulations and other public policies as they apply to an information system in a given operational environment

7. Life Cycle System Security Planning

A – Team with certifier/IA engineer to evaluate integrated logistics support cycle as it applies to IA

8. Personnel Security Policies and Guidance

I – Team with certifier/IA engineer to evaluate the implementation of established policies and procedures ensuring that personnel have required authority and appropriate clearances

9. Technical Knowledge of Information System

E – Outline technical knowledge required of personnel responsible for networks, servers, workstations, operating systems, *etc.*

10. Threat/Risk Assessment

A – Evaluate process of evaluating degree of threat to an information system

A – Evaluate process of evaluating nature of threat to an information system

11. Mission

I – Evaluate current mission and determine if an adverse system finding should be allowed to halt mission support operations

C. Effect of Countermeasure

1. Access Control Policies

I – Team with certifier/IA engineer to evaluate operating and management procedures designed to detect or prevent unauthorized access to an information system

I - Explain system IA policy with regard to the acquisition and upgrade of software and hardware components and the laws and procedures that must be observed in their implementation

2. Agency-Specific Policies and Procedures
I – Team with certifier/IA engineer to evaluate local policies and procedures that implement higher-level regulations, laws, and procedures
3. Cost/Benefit Analysis
I – Evaluate assessment of data protection costs versus loss or compromise of data
4. Countermeasures
I – Discuss actions, devices, procedures, techniques, or measures that reduce vulnerability or threat to a system
5. Life Cycle System Security Planning
I – Evaluate allowable duration of system’s operations run time, beginning with identification of a need to place a system in operation; continuing through system design, development, implementation, and operation; and ending with the system’s deactivation and disposal
6. Network Firewalls
I – Team with certifier/IA engineer to evaluate protection afforded information processed in a cryptographically-secured network
7. Preventative Controls
I – Team with certifier/IA engineer to check accuracy and reliability of an information system’s data
I – Team with certifier/IA engineer to evaluate controls to safeguard assets
I – Team with certifier/IA engineer to promote an information system’s operational efficiency
I – Team with certifier/IA engineer to encourage adherence to prescribed managerial policies
8. Security Domains
I – Explain how physical security and domains provide a useful approach for dealing with security and data protection in large-scale systems
I – Team with certifier/IA engineer to evaluate how physical security and domains provide a useful approach for dealing with security and data protection in large-scale systems
9. Security Product Testing/Evaluation
E – Examine analysis of security safeguards of a system as they have been applied to an operational environment to determine security posture
10. Technical Knowledge of Information System
E – Outline technical knowledge required of personnel responsible for operating and

maintaining networks, servers, workstations, operating systems, *etc.*

11. Technological Threats

I – Evaluate hardware, software, firmware, communication flaw, circumstance, or event with potential to cause harm to a system or data

12. Threat/Risk Assessment

I – Evaluate life cycle analysis of security requirements and countermeasures based on assessment of threats capability and motivation to exploit a vulnerability

13. Mission

A – Evaluate affects of a risk assessment and certification/accreditation process on mission of a system

FUNCTION FIVE – TESTING AND EVALUATION

Working with other IA professionals to evaluate risk mitigation through testing and evaluation.

Testing and Evaluation Duties

1. Access Authorization
I – Team with certifier/IA engineer to evaluate formal approval process and procedures for providing system access for authorized users
2. Access Privileges
I – Team with certifier/IA engineer to evaluate access permissions granted to users of system
3. Account Administration
E – Discuss maintenance of accounting files, tools, user accounts, and system statistics
4. Assessment Methodology
E – Define vulnerability analysis process
5. Associate Threat Probabilities to Vulnerability
E – Explain paired interaction of system threats and vulnerabilities
6. Audit Trails and Logging
E – Team with certifier/IA engineer to compile chronological record of system activities for reconstruction and examination of events and/or changes in an event
7. Backups
E – Discuss purpose of using copies of backup files for later reconstruction of files
8. Software Test & Evaluation Results
E – Ensure software test and evaluation results related to system restoration are performed
9. Certification
I – Assist with evaluation of technical and non-technical security features of system during testing and evaluation
10. Change Controls
I – Team with certifier/IA engineer to evaluate controls and traceability for all changes made to system during testing and evaluation

11. Client/Server Security
I – Team with certifier/IA engineer to evaluate protection schema of a distributed system that consists of workstations
12. Security Test & Evaluation Plan & Procedure
E – Assist with the development of ST&E plan and procedure for testing and evaluating a system
13. Error Logs
E – Interpret files created by operating system for review of audit process
14. Non-Technical & Technical Result
E – Interpret technical and non-technical results from testing and evaluation
15. Evaluation Techniques
E – Team with certifier/IA engineer to integrate technical analysis of components, products, subsystems, or systems security that establishes whether or not component, product subsystem, or system meets a specific set of requirements independently and in collaborative operations
16. Identify All Risk Variables
E – Explain development of a compendium of relative threats, vulnerabilities, attacks, and consequences related to a system (Common vulnerabilities and exploitations)
17. Identify Potential Corrective Approaches
I – Team with certifier/IA engineer to generate database of corrective measures to bring system into compliance of level for which being certified
18. Certification Tools
E – Team with certifier/IA engineer to interpret results of certification tools during testing and evaluation
19. Privileges (Class, Nodes)
E – Influence program or user operations that can be performed during testing and Evaluation
20. Test and Evaluation Strategies
E – Identify strengths of alternative test and evaluation strategies
I – Evaluate the relative strengths of alternative test and evaluation strategies

21. Testing Implementation of Security Features

E – Integrate testing of security features during testing and evaluation

FUNCTION SIX – THREAT AND ADVERSARY ANALYSIS

Analyzing the nature and degree of system risks.

Threat and Adversary Analysis Duties

A. General

1. Conducting Risk Analysis
E – Conduct examination of vulnerabilities, attack, threats and consequences that may affect system
2. Cost/Benefit Analysis
E – Conduct an assessment of costs of data protection for a system versus cost of loss or compromise
3. Critical Thinking
E – Discuss known and hypothetical variables based on test procedures
4. Deductive Reasoning
E – Recommend solutions based on a set of static and variable factors of system
5. Effects of Mitigation
E – Determine effects of mitigation derived from application of countermeasures to a system
6. Hostile Intelligence Sources
E – Discuss impact of hostile agents seeking national security information which could potentially cause harm to national security
7. All Risk Variables
E – Build a compendium of relative threats, vulnerabilities, attacks, and consequences related to system

B. Risk Assessment (Environment & Threat Description)

1. Risk Management Methodology
E – Discuss evaluation of threats, vulnerabilities, and countermeasures to determine residual risk
2. Security Countermeasures

E – Discuss security and software countermeasures during design, implementation, and testing phases to achieve required level of confidence

3. Threat Analysis

E – Conduct examination and evaluation of sources and factors that can adversely impact system

4. Treat Description

E – Identify level of threat based on its applicability to system

5. Threat/Risk Assessment

E – Recommend life cycle countermeasures based on assessments of threats, capabilities, and motivations to exploit vulnerability

6. Mission

E – Discuss current mission and role of information system in supporting mission

E – Determine if an adverse system finding should be allowed to halt mission support operations

7. Vulnerability Analysis

E – Appraise weaknesses in information system, security procedures, internal controls, or implementations that could be exploited

C. Analysis for Decisions

Analysis for Decisions

A – Team with certifier/IA engineer to determine countermeasures

A – Interpret system vulnerabilities

D. Agency-Specific Policies and Procedures

Agency-Specific Policies and Procedures

E – Discuss local policies and procedures implementing regulations, laws, and procedures in local environment

E. Assessment Methodology

Assessment Methodology

I – Team with certifier/IA engineer to determine method used for surveys and inspections in C&A process

I – Discuss analysis of vulnerabilities of an information system

F. Audit Trails and Logging Policies

Audit Trails and Logging Policies

- I – Discuss policies regarding audit data usage, management, and maintenance
- I – Discuss policies regarding personnel access to audit records
- I – Team with certifier to interpret guidance defining how audit collection requirements are to be implemented

G. Information Integrity

Information Integrity

- I – Discuss characteristics that ensure computer resources operate correctly
- I – Discuss characteristics that ensure data integrity
- I – Discuss security policies that describe permitted system actions
- I – Discuss security policies that describe what system actions are prohibited

H. Technical Surveillance Countermeasures

Technical Surveillance Countermeasures

- E – Discuss Techniques and measures to detect and neutralize a wide variety of hostile penetration technologies

FUNCTION SEVEN – MISSION AND ASSETS ASSESSMENTS

Determining role and criticality of information systems in supporting organizational mission.

Mission and Assets Duties

A. General

1. Conducting Risk Analysis
 - E – Conduct detailed evaluation of vulnerabilities, attack, threats, and consequences that may affect system
 - E – Conduct detailed examination of vulnerabilities, attack, threats, and consequences that may affect system
2. Cost/Benefit Analysis
 - E – Conduct cost assessment for providing data protection versus cost of data loss or compromise
3. Critical Thinking
 - E – Understand known and hypothetical variables based on test procedures
4. Deductive Reasoning
 - E – Recommend solutions based on a set of static and variable factors
5. Effects of Mitigation
 - E – Determine effects of mitigation derived from application of countermeasures
6. Hostile Intelligence Sources
 - E – Discuss impact of hostile agents seeking national security information which could potentially cause harm to national security
7. All Risk Variables
 - E – Build a compendium of relative threats, vulnerabilities, attacks, and consequences related to system

B. Risk Assessment (Environment & Threat Description)

1. Risk Management Methodology
 - E – Discuss evaluation of threats, vulnerabilities, and countermeasures to determine residual risk

2. Security Countermeasures
E – Discuss security and software countermeasures during design, implementation and testing phases to achieve required level of confidence
3. Threat Analysis
E – Conduct detailed examination and evaluation of sources and factors that can adversely impact system
I – Incorporate relevant potential threat/vulnerability information gained from available intelligence and law enforcement agency sources
4. Treat Description
E – Identify level of threat based on its applicability to system
5. Threat/Risk Assessment
E – Recommend life cycle countermeasures based on assessment of threats, capabilities, and motivations to exploit vulnerability
6. Mission
E – Assess mission to determine if an adverse finding should be allowed to affect continued IT operations in a given mission environment
7. Vulnerability Analysis
E – Appraise exploitable weaknesses in information system, security procedures, internal controls or implementations

C. Analysis for Decisions

Analysis for Decisions

- A – Interpret system vulnerabilities
- A – Determines countermeasures

D. Agency-Specific Policies and Procedures

Agency-Specific Policies and Procedures

- E – Discuss local policies and procedures implementing regulations, laws, and procedures in local environment

E. Assessment Methodology

Assessment Methodology

- I – Determine method used for surveys and inspections in C&A process
- I – Discuss analysis of vulnerabilities of an information system

F. Audit Trails and Logging Policies

Audit Trails and Logging Policies

- I – Discuss policies regarding audit data usage, management, and maintenance
- I – Discuss policies regarding personnel access to audit records
- I – Interpret guidance defining how audit collection requirements are to be implemented

G. Information Integrity

Information Integrity

- I – Define security processes that ensure computer resources operate correctly and that data in databases are correct
- I – Discuss security policy that describes types of permitted and prohibited actions on system

H. Technical Surveillance Countermeasures

Technical Surveillance Countermeasures

- E – Discuss techniques and measures to detect and neutralize hostile penetration technologies

FUNCTION EIGHT – VULNERABILITIES AND ATTACK AVENUES ANALYSIS

Evaluating system weaknesses and adversary techniques.

Vulnerability and Attack Avenues Duties

A. General

1. Vulnerabilities, attacks, threats, and consequences
E – Assess vulnerabilities, attacks, threats, and consequences to determine vulnerabilities and attack avenues
2. Cost/Benefit Analysis
E – Discuss cost analysis of data protection versus cost of data lose or compromise
3. Critical Thinking
E – Apply discrimination to known and potential vulnerabilities based on test procedures
4. Deductive Reasoning
E – Use test results to determine underlying state of system
5. Effect of Countermeasures on Risk
E – Determine effect of countermeasures on risk through the analysis of paired interaction of a defense
6. Effects of Mitigation
E – Determine effects of mitigation derived from application of countermeasures to system
7. Hostile Intelligence Sources
E – Discuss hostile intelligence sources as part of vulnerabilities and attack venues
8. Risk Variables
E – Identify risk variables to build a compendium of relative threats, vulnerabilities, attacks, and consequences related to a system
9. Jamming
E – Discuss jamming as a potential threat

10. Risk Assessment
E – Define risk assessment methodology in relation to risk analyst function
11. Risk Management Methodology
E – Define risk management methodology in relation to system security
12. Security Countermeasures
E – Discuss security countermeasures in relation to vulnerabilities and attack venues
13. Threat Analysis
E – Use threat analysis to determine vulnerabilities and attack venues
14. Threat/Risk Assessment
E – Apply threat and/or risk assessment in determining vulnerabilities and attack venues
15. Mission
E – Support organizational mission in conjunction with vulnerabilities and attack venues
16. Vulnerabilities
E – Discuss weaknesses in system, system security procedures, and internal controls and implementation
17. Vulnerability Analysis
E – Use vulnerability analysis to determine adequacy of security measures, identify security deficiencies, and provide data to predict effectiveness of security measures

B. Developing Attack Avenues

Avenues of Attack

E – Describe known avenues of attack such as operating system bugs, network vulnerabilities, human threats, *etc.*

C. Characterizing Vulnerabilities

Characterizing Vulnerabilities

E – Discuss aspects of security in a vulnerability testing and evaluation plan
E – Evaluate threats and vulnerabilities

D. Researching Vulnerability Report

Researching Vulnerability Report

E – Evaluate vulnerability assessment methodologies

E. Collecting and Reviewing Vulnerabilities

Collecting and Reviewing Vulnerabilities

E – List potential vulnerabilities that may lead to defeat of security services

I – Incorporate relevant potential vulnerability/threat information gained from intelligence and law enforcement agency sources

F. Comparing and Contrasting Attack Avenues

Comparing and Contrasting Attack Avenues

E – Discuss techniques and measures to detect or neutralize a wide variety of hostile penetration technologies

E – Evaluate payoff to and liabilities incurred by an attacker in a successful attack

I – Justify technical surveillance countermeasures

G. Risk of Detection and Response

Risk of Detection and Response

E – Characterize impact of security breaches and estimate an attacker's probable Response

H. Cost of Attack

Cost of Attack

I – Discuss return on investment results of evaluation of means by which threats can act on vulnerabilities

I – Discuss aspects of security for a system and cost incurred by an adversary to mount an attack

I. Technology Necessary to Mount Attack

Technology Necessary to Mount Attack

E – Describe technology needed to mount an attack based on existing countermeasures

FUNCTION NINE – TRAINING AND AWARENESS

Sharing IA analytical expertise and lessons learned from other IA professionals, prepare both on-line and stand-up training and awareness products.

Training and Awareness Duties

A. Policies/Procedures/Methodology

1. Access Control Policies
 - E – Summarize national and local level access control policies
 - I – Recommend implementation policies
 - I – Demonstrate effect of modification to existing access controls
 - A – Define system level access policies used to process information
2. Laws, Regulations, and Other Public Policy
 - E – Identify local application of IA laws, regulations, and policies
 - E – Discuss applicable IA laws, regulations, and policies
 - A – Explain application of IA laws, regulations, and policies
3. Agency-Specific IA and IT Policies and Procedures
 - E – Summarize agency-specific policies and procedures in relation to risk environment
 - I – Discuss agency-specific policies and procedures
 - I – Integrate agency-specific policies and procedures into results of risk analysis report
4. Assessment Methodology
 - I – Assist in integration of a variety of assessment methodologies into curricula
 - A – Provide interpretation of strengths and weaknesses of assessment methodologies
5. Audit Trails and Logging Policies
 - E – Discuss audit trails and logging policies
 - I – Provide audit trail and logging policy examples for training
 - I – Explain role of audit trails
6. Change Control Policies
 - E – Discuss change control policies for incorporation in IA training
 - I – Explain change control policies for incorporation in IA training
 - I – Influence change control policies in corporation in IA training
7. Communications Security Policy and Guidance
 - A – Interpret communications security policy and guidance for incorporation into IT

- training
E – Discuss communications security policy and guidance for incorporation into IT training
training
E – Identify communications security policy and guidance for incorporation into IT training
training
I – Explain communications security policy and guidance for incorporation into IT training
8. Emergency Destruction Planning and Procedures (EDPP)
E – Discuss EDPP for incorporation in IA training
I – Explain EDPP for incorporation in IA training
 9. Personnel Security Policies and Guidance
E – Discuss role of personnel security policies and guidance as part of overall risk management plan
 10. Formal Methods for Security Design
E – Outline role of formal methods in security design as part of risk management plan
 11. Information Categorization
E – Discuss various categorization schemas
I – Explain role of information categorization schema as part of risk management plan
 12. Information Classification
E – Discuss classification policies as part of risk management plan
I – Explain classification policies as part of risk management plan
 13. Knowledge and/or Awareness of Security Laws
I – Outline security laws and applicability to risk management plan
 14. Methods of Defining Security Requirements
E – Discuss definitions of security requirements
I – Compare and contrast various methods for defining security requirements
 15. Physical Security Requirements
E – Discuss physical security requirements
I – Summarize physical security requirements
 16. Risk Acceptance Process
I – Explain risk acceptance process to include mitigation versus avoidance

17. Risk Management Methodology
E – Summarize approaches to risk management
18. Security Awareness
I – Explain role of security awareness as part of risk management plan
19. Ethics
I – Give examples of lessons learned in ethical/unethical cyber behavior and relate to risk management plan

B. Technology

1. Applications Security
E – Discuss state of security features embedded in commercial-off-the-shelf (COTS) products in relation to risk management plan
2. Database Security Features
E – Discuss elements of database security features
E – Identify critical database security pitfalls
E – List database best practices and pitfalls in database security
3. Distributed Systems Security
E – Discuss risks associated with distributed systems security
4. Firmware Security
E – Discuss differences between security features and capabilities
5. Industrial Security
I – Explain rules and measures in place for implementing IA measures with industrial partners/contractors
6. Multi-Discipline Security
I – List relations between variety of disciplines employed in IA
I – Explain relations between variety of disciplines employed in IA
7. Network Security Software
E – Discuss state and vulnerabilities in network security software
8. Remanence
I – Explain threats and vulnerabilities associated with remanence

9. Technology Trends

E – Summarize technology trends in context of future security management plan

10. Environmental/Natural Threats

E – List environmental and natural threats as part of security management plan

E – Discuss environmental and natural threats as part of security management plan

ANNEX B

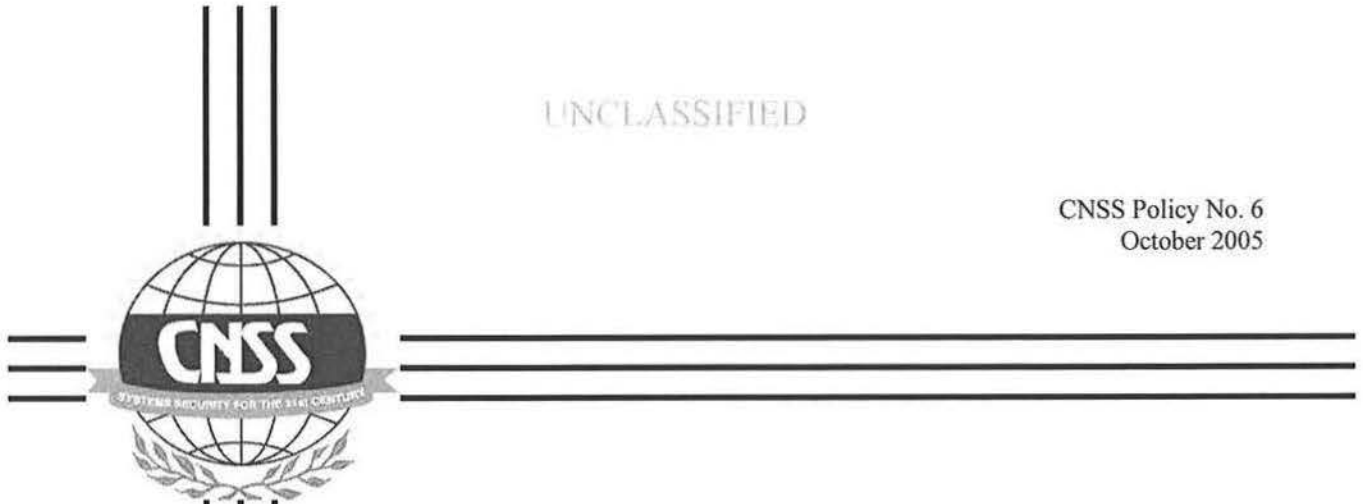
REFERENCES

- a. CNSS Instruction No. 4009, "National Information Assurance (IA) Glossary," dated 19 May 2003.
- b. NSTISS Directive No. 501, "National Training Program for Information Systems Security (INFOSEC) Professionals," dated 16 November 1992.
- c. "The National Strategy to Secure Cyberspace, Priority III: A National Cyberspace Security Awareness and Training Program," dated February 2003.
- d. "Federal Information Security Management Act of 2002 (FISMA)," contained under Title III of the "Electronic Government Act," dated December 17, 2002.
- e. NSTISS Instruction No. 4011, "National Training Standard for Information Systems Security (INFOSEC) Professionals," dated 20 June 1994.
- f. NSTISS Instruction No. 4015, "National Training Standard for Systems Certifiers," dated December 2000.
- g. CNSS Instruction No. 4012, "National Information Assurance Training Standard for Senior System Managers, dated June 2004.
- h. CNSS Instruction No. 4103, "National Information Assurance Training Standard for System Administrators (SA)," dated March 2004.
- i. CNSS Instruction No. 4014, "National Information Assurance Training Standard for Information Systems Security Officers," dated April 2004.

H. National Policy on Certification and Accreditation of National Security Systems

UNCLASSIFIED

CNSS Policy No. 6
October 2005



**NATIONAL POLICY
ON
CERTIFICATION AND ACCREDITATION
OF
NATIONAL SECURITY SYSTEMS**

UNCLASSIFIED

UNCLASSIFIED

CNSS Policy No. 6



Committee on National Security Systems

FOREWORD

1. The national security community, in order to ensure the security of National Security Systems, is developing cost-effective policies, procedures, and methodologies for the certification and accreditation (C&A) of national telecommunications and information systems. This C&A policy for National Security Systems will begin to provide the community with standard methodologies for C&A processes, assign authority and responsibilities, and lay a basis for mutual recognition of certification results. This policy supersedes NSTISSP Policy No. 6, "National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems," dated 8 April 1994.

2. Representatives of the Committee on National Security Systems (CNSS) may obtain additional copies of this policy at the address below.

3. U.S. Government contractors are to contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.

/s/
Linton Wells II

(410) 854-6805 . UFAX: (410) 854-6814

cnss@radium.ncsc.mil

UNCLASSIFIED

**NATIONAL POLICY
ON
CERTIFICATION AND ACCREDITATION OF NATIONAL SECURITY SYSTEMS**

SECTION I - POLICY

1. All federal government departments and agencies shall establish and implement programs that mandate the certification and accreditation (C&A) of National Security Systems (NSS) under their operational control. These C&A programs shall ensure that information collected, generated, processed, stored, displayed, transmitted or received by NSS is adequately protected with respect to requirements for confidentiality, integrity, and availability. NTISSI No. 1000, "National Information Assurance Certification and Accreditation Process (NIACAP)" was developed to provide minimum standards for the certification and accreditation of national security systems. Federal departments and agencies shall refer to the NIACAP, or a C&A process that is consistent with the NIACAP, when developing their C&A programs.

2. Nothing in this policy alters or supersedes the existing authorities of the Director of National Intelligence.

SECTION II - DEFINITIONS

3. The following definitions were taken from CNSSI No. 4009, National Information Assurance (IA) Glossary unless otherwise noted.

a. Accreditation - Formal declaration by a Designated Approving Authority (DAA) that an information system (IS) is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. (C&A Working Group definition.)

b. Certification - Comprehensive evaluation of the technical and non-technical security safeguards of an IS to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.

c. Designated Approving Authority (DAA) - Official with the authority to formally assume the responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority.

d. Information System (IS) - Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.

e. National Security System (NSS) - Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency,

(1) the function, operation, or use of which:

involves intelligence activities;

involves cryptologic activities related to national security;

involves command and control of military forces;

involves equipment that is an integral part of a weapon or weapon system;

or

(subject to Subparagraph (B)*) is critical to the direct fulfillment of military or intelligence missions; or

(2) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

*Subparagraph B – Does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (Title 44 U.S.C. 3542, Federal Information Security Management Act of 2002)

f. Telecommunications - Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.

SECTION III - PRINCIPLES

4. C&A programs established to satisfy this policy shall be based on the following principles:

a. Certification of NSS shall be performed and documented in accordance with specified criteria, standards, and guidelines.

b. All NSS shall be accredited by DAAs. The DAA shall be in a position to balance operational mission requirements and the residual risk of system operations, and to understand the risk of accepting interconnection to other systems and networks outside of the DAA's authority. All accreditation decisions shall be documented and contain a statement of residual risk.

c. Departments and agencies shall freely exchange technical C&A information, coordinate programs, and participate in cooperative projects wherever possible consistent with the classification and sensitivity of the C&A information and results.

d. To promote cost-effective security across the federal government, department and agency programs for the C&A of NSS shall be developed in concert with similar programs that address the security of non-NSS.

e. As cornerstones of a continuous process of effective security management, activities in support of C&A shall be performed throughout the total system life cycle.

SECTION IV - RESPONSIBILITIES

5. Heads of U.S. Government departments and agencies shall:

a. ensure their C&A program is consistent with the policy and principles set forth in this CNSS policy,

b. ensure that a DAA is appointed for each system under their operational control and

c. ensure that the appointed DAA is aware of his or her responsibilities as outlined in CNSSI No. 4012, " National Information Assurance Training Standard for Senior System Managers."

6. The National Manager for the CNSS, in coordination with CNSS members and others as appropriate, shall develop and promulgate minimum technical criteria, standards, and guidelines for the certification and accreditation of NSS.



FACT SHEET

NSTISSP No. 11, Revised Fact Sheet **National Information Assurance Acquisition Policy** *(Includes deferred compliance guidelines and procedures)*

July 2003

Background

(1) National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, Subject: National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products was issued by the National Security Telecommunications and Information Systems Security Committee (NSTISSC), now known as the Committee on National Security Systems (CNSS), in January 2000 and revised in June 2003.

(2) The Committee was established by National Security Directive (NSD) No. 42, dated July 1990, and is responsible for developing and promulgating national policies applicable to the security of national security telecommunications and information systems.

Introduction

(3) The technological advances and threats of the past decade have drastically changed the way we think about protecting our communications and communications systems. Three factors are of particular significance:

- The need for protection encompasses more than just confidentiality;
- Commercial Off-the-Shelf (COTS) security and security-enabled IA products are readily available as alternatives to traditional NSA-developed and produced communications security equipment (i.e., Government-Off-the Shelf (GOTS) products); and
- An increased and continuing recognition that the need for IA transcends more than just the traditional national security applications of the past.

(4) In the context of the second sub-bullet of paragraph (3), it is important that COTS products acquired by U.S. Government Departments and Agencies be subject to a standardized evaluation process, which will provide some assurances that these products perform as advertised. Accordingly, NSTISSP No. 11 has been developed as a means of addressing this problem for those products acquired for national security applications. NSTISSP No. 11 also rightfully points out that protection of systems encompasses more than just acquiring the right product. Once acquired, these products must be integrated properly and subject to an accreditation process, which will ensure total integrity of the information and systems to be protected.

Policy

(5) IA shall be considered as a requirement for all systems used to enter, process, store, display, or transmit national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated GOTS or COTS IA and IA-enabled IT products. These products should provide for the availability of the systems, ensure the integrity and confidentiality of information, and ensure the authentication and non-repudiation of parties in electronic transactions.

(6) On 1 January 2001, preference was to be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting national security information) which had been evaluated and validated, as appropriate, in accordance with:

- The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement;
- The National Security Agency (NSA) /National Institute of Standards and Technology (NIST) National Information Assurance Partnership (NIAP) Evaluation and Validation Program; or
- The NIST Federal Information Processing Standard (FIPS) validation program.

(7) Effective 1 July 2002, the acquisition of all COTS IA and IA-enabled IT products to be used on the systems specified in paragraph (6), shall be limited only to those which have been evaluated and validated in accordance with the criteria, schemes, or programs specified in the three sub-bullets of paragraph (6).

(8) The evaluation/validation of COTS IA and IA-enabled IT products will be conducted by accredited commercial laboratories, or the NIST.

(9) The acquisition of all GOTS IA and IA-enabled products to be used on systems entering, processing, storing, displaying, or transmitting national security information

shall be limited to products which have been evaluated by NSA, or in accordance with NSA-approved processes.

(10) Normally, a complementary combination of IA/IA-enabled products is needed to provide a complete security solution to a given environment. Thus, in addition to employing evaluated and validated IA/IA-enabled products, a solution security analysis should be conducted as part of the certification and accreditation process. In support of this, NSA shall provide guidance regarding the appropriate combinations and implementation of GOTS and COTS IA and IA-enabled products.

(11) Subject to policy and guidance for non-national security systems, departments and agencies may wish to consider the acquisition and appropriate implementation of evaluated and validated COTS IA and IA-enabled IT products. The use of these products may be appropriate for systems which process, store, display, or transmit information that, although not classified, may be critical or essential to the conduct of organizational missions, or for information or systems which may be associated with the operation and/or maintenance of critical infrastructures as defined in Presidential Decision Directive No. 63 (PDD-63), Critical Infrastructure Protection, dated 22 May 1998.

Responsibilities

(12) Heads of U.S. Departments and Agencies are responsible for ensuring compliance with the requirements of this policy.

Exemptions and Deferred Compliance

(13) COTS or GOTS IA and IA-enabled IT products acquired prior to the effective dates prescribed herein shall be exempt from the requirements of this policy. Information systems in which those products are integrated should be operated with care and discretion and evaluated/validated IA products and solutions considered as replacement upgrades at the earliest opportunity.

(14) While COTS IA and IA-enabled products (non-encryption based) have been developed, evaluated, and are available for acquisition and implementation on national security systems, it is recognized that these products do not cover the full range of potential user applications. Rapid technologic changes and the amount of time it takes to successfully complete a product evaluation also affect compliance with NSTISSP No. 11. Therefore, full and immediate compliance with NSTISSP No. 11 may not be possible for all acquisitions.

(15) No blanket or open-ended waivers to NSTISSP No. 11 will be authorized, but a Deferred Compliance Authorization (DCA)¹ may be granted on a case-by-case basis.

¹ A **Deferred Compliance Authorization (DCA)** is a formal approval by an authorized official to defer compliance with the requirements of a national IA policy for a specified period of time, normally not to exceed more than one calendar year.

Departments and agencies electing to pursue a DCA from the policy requirements of NSTISSP No. 11, shall use the following guidelines when determining whether a DCA is appropriate for a particular application and, if so, who has the authority for reviewing and approving a requested DCA.

Deferred Compliance Guidance

(16) The issuance of a DCA will apply only to environments not requiring the encryption of classified information. A DCA will not be submitted for encryption products. Encryption products for protecting classified information will be certified by NSA, and encryption products intended for protecting sensitive information will be certified in accordance with NIST FIPS 140-2.

(17) A DCA is applicable only to the acquisition of a specific COTS product for a specific application within the IT enterprise of an organization. It does not constitute blanket approval for future acquisitions of the same product and does not obviate the requirement for the requesting organization to obtain necessary certification and accreditation approval for the application or system in which the product will be used prior to operational use. A record of all DCAs will be included in certification and accreditation documentation.

(18) A DCA will be reviewed and approved only by the heads of federal departments or agencies, or major subordinate organizations with a department or agency (e.g., the Defense Intelligence Agency (DIA) within the Department of Defense). Heads of departments or agencies (or major subordinate organizations) may delegate their DCA review and approval authorities to a designee within their respective organizations. This normally would be the Chief Information Officer (CIO) or equivalent, or any other individual responsible for the security of the overall IT enterprise within that department or agency. Delegations of DCA authority must be formalized in writing and their currency maintained.

Deferred Compliance Procedures

(19) Those individuals or organizations (These could include IA/IT planners, designers, integrators, as well as acquisition entities.) responsible for IA within their respective departments or agencies will determine whether an evaluated product (or products) is available to satisfy a particular requirement.

(20) If an evaluated product is not available, DCA documentation will be prepared and submitted to the DCA approving authority. The DCA documentation must contain the following information:

- A description of the intended application and type of product needed;
- Details of why an evaluated product is not being procured (e.g., no products of this type have been evaluated, or an explanation as to why available evaluated products do not meet user's functional or security requirements);
- Product information, ideally the product's Security Target (i.e., the security claims being made by the vendor), and evidence (as documented by an appropriate department or agency testing facility) that the product's features and assurances are adequate for the intended application;
- The product quantity that is being acquired; and
- A statement that the requesting department or agency will, as a condition of purchase, require the product and its associated Security Target to be submitted for evaluation and validation to a Common Criteria Testing Laboratory accredited by the NSA/NIST NIAP Evaluation and Validation Program or a member nation recognized under the International Common Criteria for Information Technology Security Evaluation Security Mutual Recognition Arrangement.

(21) The Certifiers and Accreditors of systems that are relying on the security features and assurances of a product submitted and approved for a DCA should recognize that the security claims of the product have yet to be independently validated and therefore, should consider issuing Interim Approval to Operate (IATO) rather than Approval to Operate (ATO) for these systems.

(22) In the event an installed product fails to meet established validation and certification testing requirements during the period of the authorized DCA, it is recommended that Certifiers and Accreditors take steps to remove the product from national security systems falling under their purview. As with any security decision, the CIO (or equivalent authority) has the option of authorizing continued use of the failed product and accepting the risk of continued use, but should mandate follow-on actions that will ensure that the product is evaluated and validated for use on a national security system. Such "continue to operate" decisions should be formally documented and included in the overall system certification and accreditation documentation.

(23) The DCA approving authority will review and approve the DCA and submit the DCA documentation to the CNSS Secretariat through the Information Assurance Directorate (IAD) of the National Security Agency:

National Security Agency

ATTN: V1
Suite 6740
Ft. George G. Meade, MD 20755-6740

V1 may also be contacted via commercial phone at 410-545-4384 or fax at 410-854-6615.



Department of Defense

DIRECTIVE

NUMBER 8500.01/1

October 24, 2002

Certified Current as of April 23, 2007

ASD(NII)/DoD CIO

SUBJECT: Information Assurance (IA)

- References: (a) Section 2224 of title 10, United States Code, "Defense Information Assurance Program"
- (b) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988 (hereby canceled)
 - (c) DoD 5200.28-M, "ADP Security Manual," January 1973 (hereby canceled)
 - (d) DoD 5200.28-STD, "DoD Trusted Computer Security Evaluation Criteria," December 1985 (hereby canceled)
 - (e) through (a/h), see enclosure 1

1. PURPOSE

This Directive:

1.1. Establishes policy and assigns responsibilities under reference (a) to achieve Department of Defense (DoD) information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare.

1.2. Supersedes DoD Directive 5200.28, DoD 5200.28-M, DoD 5200.28-STD, and DoD Chief Information Officer (CIO) Memorandum 6-8510 (references (b), (c), (d), and (e)).

1.3. Designates the Secretary of the Army as the Executive Agent for the integration of common biometric technologies throughout the Department of Defense.

1.4. Authorizes the publication of DoD 8500.1-M consistent with DoD 5025.1-M (reference (f)).

2. APPLICABILITY AND SCOPE

2.1. This Directive applies to:

2.1.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

2.1.2. All DoD-owned or -controlled information systems that receive, process, store, display or transmit DoD information, regardless of mission assurance category, classification or sensitivity, including but not limited to:

2.1.2.1. DoD information systems that support special environments, e.g., Special Access Programs (SAP) and Special Access Requirements (SAR), as supplemented by the special needs of the program.

2.1.2.2. Platform IT interconnections, e.g., weapons systems, sensors, medical technologies or utility distribution systems, to external networks.

2.1.2.3. Information systems under contract to the Department of Defense.

2.1.2.4. Outsourced information-based processes such as those supporting e-Business or e-Commerce processes.

2.1.2.5. Information systems of Nonappropriated Fund Instrumentalities.

2.1.2.6. Stand-alone information systems.

2.1.2.7. Mobile computing devices such as laptops, handhelds, and personal digital assistants operating in either wired or wireless mode, and other information technologies as may be developed.

2.2. Nothing in this policy shall alter or supercede the existing authorities and policies of the Director of Central Intelligence (DCI) regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence as directed by Executive Order 12333 (reference (g)) and other laws and regulations.

2.3. This policy does not apply to weapons systems as defined by DoD Directive *51-14.1* (reference (h)) or other IT components, both hardware and software, that are physically part of, dedicated to, or essential in real time to a platform's mission performance where there is no platform IT interconnection.

3. DEFINITIONS

Terms used in this Directive are defined in National Security Telecommunications and Information Systems Security Instruction Number 4009 (reference (i)) or enclosure 2.

4. POLICY

It is DoD policy that:

4.1. Information assurance requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DoD information systems in accordance with 10 U.S.C. Section 2224, Office of Management and Budget Circular A-130, Appendix III, DoD Directive 5000.1 (references (a), (j), and (k)), this Directive, and other IA-related DoD guidance, as issued.

4.2. All DoD information systems shall maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability that reflect a balance among the importance and sensitivity of the information and information assets; documented threats and vulnerabilities; the trustworthiness of users and interconnecting systems; the impact of impairment or destruction to the DoD information system; and cost effectiveness. For IA purposes all DoD information systems shall be organized and managed in the four categories defined in enclosure 2: automated information system (AIS) applications, enclaves (which include networks), outsourced IT-based processes, and platform IT interconnections.

4.3. Information assurance shall be a visible element of all investment portfolios incorporating DoD-owned or -controlled information systems, to include outsourced business processes supported by private sector information systems and outsourced information technologies; and shall be reviewed and managed relative to contributions to mission outcomes and strategic goals and objectives, in accordance with 40 U.S.C. Sections 1423 and 1451 (reference (l)). Data shall be collected to support reporting and IA management activities across the investment life cycle.

4.4. Interoperability and integration of IA solutions within or supporting the Department of Defense shall be achieved through adherence to an architecture that will enable the evolution to network centric warfare by remaining consistent with the Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance Architecture Framework, and a defense-in-depth approach. This combination produces layers of technical and non-technical solutions that: provide appropriate levels of confidentiality, integrity, authentication, non-repudiation, and availability; defend the perimeters of enclaves; provide appropriate degrees of protection to all enclaves and computing environments; and make appropriate use of supporting IA infrastructures, to include robust key management and incident detection and response.

4.5. The Department of Defense shall organize, plan, assess, train for, and conduct the defense of DoD computer networks as integrated computer network defense (CND) operations that are coordinated across multiple disciplines in accordance with DoD Directive O-8530.1 (reference (m)).

4.6. Information assurance readiness shall be monitored, reported, and evaluated as a distinguishable element of mission readiness throughout all the DoD Components, and validated by the DoD CIO.

4.7. All DoD information systems shall be assigned a mission assurance category that is directly associated with the importance of the information they contain relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Requirements for availability and integrity are associated with the mission assurance category, while requirements for confidentiality are associated with the information classification or sensitivity and need-to-know. Both sets of requirements are primarily expressed in the form of IA controls and shall be satisfied by employing the tenets of defense-in-depth for layering IA solutions within a given IT asset and among assets; and ensuring appropriate robustness of the solution, as determined by the relative strength of the mechanism and the confidence that it is implemented and will perform as intended. The IA solutions that provide availability, integrity, and confidentiality also provide authentication and non-repudiation.

4.8. Access to all DoD information systems shall be based on a demonstrated need-to-know, and granted in accordance with applicable laws and DoD 5200.2-R (reference (n)) for background investigations, special access and IT position designations and requirements. An appropriate security clearance and non-disclosure agreement are also required for access to classified information in accordance with DoD 5200.1-R (reference (o)). Further:

4.8.1. The minimum requirement for DoD information system access shall be a properly administered and protected individual identifier and password.

4.8.2. The use of Public Key Infrastructure (PKI) certificates and biometrics for positive authentication shall be in accordance with published DoD policy and procedures. These technologies shall be incorporated in all new acquisitions and upgrades whenever possible. Where interoperable PKI is required for the exchange of unclassified information with vendors and contractors, the Department of Defense shall only accept PKI certificates obtained from a DoD-approved external certificate authority or other mechanisms approved in accordance with DoD policy.

4.9. In addition to the requirements in paragraph 4.8., foreign exchange personnel and representatives of foreign nations, coalitions or international organizations may be authorized access to DoD information systems containing classified or sensitive information only if all of the following conditions are met:

4.9.1. Access is authorized only by the DoD Component Head in accordance with the Department of Defense, the Department of State (DoS), and DCI disclosure and interconnection policies, as applicable.

4.9.2. Mechanisms are in place to strictly limit access to information that has been cleared for release to the represented foreign nation, coalition or international organization, (e.g., North Atlantic Treaty Organization) in accordance with DoD Directive 5230.11 (reference (p)), for classified information, and other policy guidance for unclassified information such as reference (o), DoD Directive 5230.20~~E~~ (reference (q)), and DoD Instruction 5230.27 (reference (r)).

4.10. Authorized users who are contractors, DoD direct or indirect hire foreign national employees, or foreign representatives as described in paragraph 4.9., above, shall always have their affiliation displayed as part of their e-mail addresses.

4.11. Access to DoD-owned, -operated or -outsourced web sites shall be strictly controlled by the web site owner using technical, operational, and procedural measures appropriate to the web site audience and information classification or sensitivity.

4.11.1. Access to DoD-owned, -operated or -controlled web sites containing official information shall be granted according to reference (o) and need-to-know rules established by the information owner.

4.11.2. Access to DoD-owned, -operated or -controlled web sites containing public information is not restricted; however, the information accessible through the web sites shall be limited to unclassified information that has been reviewed and approved for release in accordance with DoD Directive 5230.9 and DoD Instruction 5230.29 (references (s) and (t)).

4.12. DoD information systems shall regulate remote access and access to the Internet by employing positive technical controls such as proxy services and screened subnets, also called demilitarized zones (DMZ), or through systems that are isolated from all other DoD information systems through physical means. This includes remote access for telework.

4.13. All DoD information systems shall be certified and accredited in accordance with DoD Instruction 5200.40 (reference (u)).

4.14. All interconnections of DoD information systems shall be managed to continuously minimize community risk by ensuring that the assurance of one system is not undermined by vulnerabilities of interconnected systems.

4.14.1. Interconnections of Intelligence Community (IC) systems and DoD information systems shall be accomplished using a process jointly established by the DoD CIO and the IC CIO.

4.14.2. Connection to the Defense Information System Network (DISN) shall comply with connection approval procedures and processes, as established.

4.14.3. Interconnections among DoD information systems of different security domains or with other U.S. Government systems of different security domains shall be employed only to meet compelling operational requirements, not operational convenience. Secure configurations of approved IA and IA-enabled IT products, uniform risk criteria, trained systems security personnel, and strict configuration control shall be employed. The community risk shall be assessed and measures taken to mitigate that risk in accordance with procedures established by the DISN Designated Approving Authorities (DAAs) prior to interconnecting the systems.

4.14.4. The interconnection of DoD information systems with those of U.S. allies, foreign nations, coalition partners, or international organizations shall comply with applicable international agreements and, whenever possible, DoD IA policies. Variations shall be approved by the responsible Combatant Commander and the DISN DAAs, and incorporated in the system security documentation. Information provided through these interconnections must be released in accordance with reference (o) or reference (p).

4.15. All DoD information systems shall comply with DoD ports and protocols guidance and management processes, as established.

4.16. The conduct of all DoD communications security activities, including the acquisition of COMSEC products, shall be in accordance with DoD Directive C-5200.5 (reference (v)).

4.17. All IA or IA-enabled IT hardware, firmware, and software components or products incorporated into DoD information systems must comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy Number 11 (reference (w)). Such products must be satisfactorily evaluated and validated either prior to purchase or as a condition of purchase; i.e., vendors will warrant, in their responses to a solicitation and as a condition of the contract, that the vendor's products will be satisfactorily validated within a period of time specified in the solicitation and the contract. Purchase contracts shall specify that product validation will be maintained for updated versions or modifications by subsequent evaluation or through participation in the National IA Partnership (NIAP) Assurance Maintenance Program.

4.18. All IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines.¹

4.19. Public domain software products, and other software products with limited or no warranty, such as those commonly known as freeware or shareware, shall only be used in DoD information systems to meet compelling operational requirements. Such products shall be thoroughly assessed for risk and accepted for use by the responsible DAA.

¹ Guidelines are available at <http://iase.disa.mil/> and <http://www.nsa.gov/>

4.20. DoD information systems shall be monitored based on the assigned mission assurance category and assessed risk in order to detect, isolate, and react to intrusions, disruption of services, or other incidents that threaten the IA of DoD operations or IT resources, including internal misuse. DoD information systems also shall be subject to active penetrations and other forms of testing used to complement monitoring activities in accordance with DoD and Component policy and restrictions.

4.21. Identified DoD information system vulnerabilities shall be evaluated for DoD impact, and tracked and mitigated in accordance with DoD-directed solutions, e.g., Information Assurance Vulnerability Alerts.

4.22. All personnel authorized access to DoD information systems shall be adequately trained in accordance with DoD and Component policies and requirements and certified as required in order to perform the tasks associated with their IA responsibilities.

4.23. Individuals shall be notified of their privacy rights and security responsibilities in accordance with DoD Component General Counsel-approved processes when attempting access to DoD information systems.

4.24. Mobile code technologies shall be categorized and controlled to reduce their threat to DoD information systems in accordance with DoD and Component policy and guidance.

4.25. A DAA shall be appointed for each DoD information system operating within or on behalf of the Department of Defense, to include outsourced business processes supported by private sector information systems and outsourced information technologies. The DAA shall be a U.S. citizen, a DoD employee, and have a level of authority commensurate with accepting, in writing, the risk of operating DoD information systems under his or her purview.

4.26. All military voice radio systems, to include cellular and commercial services, shall be protected consistent with the classification or sensitivity of the information transmitted on the system.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for *Networks and Information Integration*, as the DoD Chief Information Officer, shall:

5.1.1. Monitor, evaluate and provide advice to the Secretary of Defense regarding all DoD IA activities.

5.1.2. Oversee appropriations earmarked for the DoD IA program and manage the supporting activities of the office of the Defense-wide Information Assurance Program (DIAP) Office in accordance with reference (a).

5.1.3. Develop and promulgate additional IA policy guidance consistent with this Directive to address such topics as ports and protocols management, vulnerability management, biometrics, security management, IA education and training, mobile code, and interconnection between security domains.

5.1.4. Ensure the integration of IA initiatives with critical infrastructure protection sector liaisons, as defined in DoD Directive ~~3020.40~~ (reference (x)).

5.1.5. Establish a formal coordination process with the IC CIO to ensure proper protection of IC information within the Department of Defense.

5.1.6. Establish metrics and annually validate the IA readiness of all DoD Components as an element of mission readiness.

5.1.7. Ensure that responsibilities for IA aspects of Major Defense Acquisition Program design are integrated into existing Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) and Service Acquisition Executive processes.

5.1.8. Require the Director, Defense Information Systems Agency (DISA) to:

5.1.8.1. Develop, implement and oversee a single IA approach for layered protection (defense-in-depth) of the DISN in coordination with the Chairman of the Joint Chiefs of Staff, Director, Defense Intelligence Agency (DIA) and Director, National Security Agency (NSA).

5.1.8.2. Establish and manage connection approval processes for the DISN.

5.1.8.3. Develop and provide IA training and awareness products.

5.1.8.4. Develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA.

5.1.8.5. Establish and implement:

5.1.8.5.1. A DoD ports and protocols management process.

5.1.8.5.2. Procedures for mitigation of risks associated with the use of mobile code in DoD information systems.

5.1.8.5.3. A web-based resource providing access to current DoD and Federal IA and IA-related policy and guidance, including recent and pending legislation.

5.1.9. Require the Director, Defense Intelligence Agency to:

5.1.9.1. Provide finished intelligence on IA, including threat assessments, to the DoD Components.

5.1.9.2. Develop, implement, and oversee an IA program for layered protection of the DoD non-cryptologic SCI systems including the DoD Intelligence Information System (DoDIIS) on the basis of defined DoD information systems and geographical or organizational boundaries.

5.1.9.3. Certify and accredit DoD non-cryptologic SCI and DoDIIS applications, enclaves, platform IT interconnections, and outsourced IT-based processes, and develop and provide an IA education, training, and awareness program for DoD non-cryptologic SCI systems and DoDIIS users and administrators.

5.1.9.4. Establish and manage a connection-approval process for the Joint Worldwide Intelligence Communications System.

5.1.10. Require the Director, Defense Security Service to monitor information system security practices and conduct regular inspections of DoD contractors processing classified information in accordance with DoD 5220.22-M (reference (y)).

5.2. The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) shall:

5.2.1. Require the Director, Defense Research and Engineering (DDR&E) to:

5.2.1.1. Monitor and oversee, in coordination with the Defense-wide Information Assurance Program Office, all Defense-wide IA research and technology investments and activities to include protection mechanisms, detection and monitoring, response and recovery, and IA assessment tools and techniques.

5.2.1.2. Require the Director, Defense Advanced Research Projects Agency (DARPA) to coordinate all DoD IA research and technology initiatives under DARPA's purview with the Director, NSA.

5.2.2. Integrate policies established by this Directive and reference (w) into acquisition policy and guidance to include the Federal Acquisition Regulations System (reference (z)), and incorporate such policies into acquisitions under his or her purview.

5.2.3. Oversee IA assessments, in coordination with the Director, Operational Testing and Evaluation.

5.3. The Under Secretary of Defense for Personnel and Readiness shall, in coordination with the ASD(VII), develop and implement IA personnel management and skill tracking procedures and processes to ensure adequate personnel resources are available to meet critical DoD IA requirements.

5.4. The OSD Principal Staff Assistants shall:

5.4.1. Ensure end-to-end protection of information flows in their functional areas by guiding investments and other actions relating to IA.

5.4.2. Ensure that IA requirements for DoD information systems developed under their cognizance are fully coordinated at the DoD Component level and with the DIAP.

5.4.3. Appoint DAAs for Joint and Defense-wide information systems under their purview (e.g., the Defense Civilian Personnel Data System, Defense Message System, Defense Travel System, and the Joint Total Asset Visibility System).

5.4.4. Identify and include IA requirements in the design, acquisition, installation, operation, upgrade or replacement of all DoD information systems under their purview.

5.5. The Secretary of the Army shall serve as the Executive Agent for the integration of common biometric technologies throughout the Department of Defense.

5.6. The Chairman of the Joint Chiefs of Staff shall:

5.6.1. Serve as the principal military advisor to the Secretary of Defense on IA.

5.6.2. Ensure, in coordination with the ASD(VII), the validation of IA requirements for systems supporting Joint and Combined operations through the Joint Requirements Oversight Council.

5.6.3. Develop, coordinate, and promulgate IA policies, doctrine and procedures for Joint and Combined operations.

5.7. The Commander, United States Strategic Command, shall coordinate and direct DoD-wide CND operations in accordance with reference (m).

5.8. The Director, National Security Agency (NSA), shall:

5.8.1. Implement an IA intelligence capability responsive to requirements for the Department of Defense, less DIA responsibilities.

5.8.2. Provide IA support to the DoD Components as required in order to assess the threats to, and vulnerabilities of, information technologies.

5.8.3. Serve as the DoD focal point for IA cryptographic research and development in accordance with DDR&E direction and in coordination with the Director, DARPA.

5.8.4. Manage the development of the IA Technical Framework (reference (a)) in support of defense-in-depth, and provide engineering support and other technical assistance for its implementation within the Department of Defense.

5.8.5. Serve as the DoD focal point for the NIAP and establish criteria and processes for evaluating and validating all IA and IA-enabled IT products used in DoD information systems.

5.8.6. Plan, design, and manage the implementation of the Key Management Infrastructure/PKI within the Department of Defense.

5.8.7. In coordination with the USD(AT&L), develop and maintain an information system security engineering process that supports IT acquisition.

5.8.8. Support the Director, Defense Information Systems Agency in the development of security configuration guidance for IA and IA-enabled IT products.

5.8.9. Develop, implement, and oversee an IA program for layered protection of DoD cryptologic SCI systems, an IA certification and accreditation process for DoD cryptologic SCI applications, enclaves, platform IT interconnections and outsourced IT-based processes, and an IA education, training, and awareness program for users and administrators of DoD cryptologic SCI systems.

5.9. The Director, Operational Testing and Evaluation, shall oversee IA assessments.

5.10. The Heads of the DoD Components shall:

5.10.1. Develop and implement an IA program focused on assurance of DoD Component-specific information and systems (e.g., sustaining base, tactical, and Command, Control, Communications, Computers, and Intelligence (C4I) interfaces to weapon systems) that is consistent with references (a) and (l) and defense-in-depth.

5.10.2. Coordinate with Joint and Defense-wide program offices to ensure interoperability of IA solutions across the DoD enterprise.

5.10.3. Collect and report IA management, financial, and readiness data to meet DoD IA internal and external reporting requirements.

5.10.4. Appoint DAAs for all DoD information systems for which they have responsibility.

5.10.5. Identify and include IA requirements in the design, acquisition, installation, operation, upgrade or replacement of all DoD information systems for which they have responsibility.

5.10.6. Ensure that the Government's contract requirements properly reflect that IA or IA-enabled IT products are involved and must be properly evaluated and validated in accordance with paragraph 4.17., above.

5.10.7. Ensure that IA awareness, training, education, and professionalization are provided to all Component personnel commensurate with their respective responsibilities for developing, using, operating, administering, maintaining, and retiring DoD information systems.

5.10.8. Comply with established accreditation and connection approval processes required for all DoD information systems.

5.10.9. Coordinate all IA research and technology initiatives under their purview with the DDR&E.

6. EFFECTIVE DATE

This Directive is effective immediately.



Paul Wolfowitz
Deputy Secretary of Defense

Enclosures - 2

E1. References, continued

E2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

- (e) DoD CIO Memorandum 6-8510, "Guidance and Policy for Department of Defense Global Information Grid Information Assurance," June 16, 2000 (hereby canceled)
- (f) DoD 5025.1-M, "DoD Directives System Procedures," *March 5, 2003*
- (g) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
- (h) DoD Directive *5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005*
- (i) National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, "National Information Systems Security Glossary," September 2000²
- (j) OMB Circular A-130, "Management of Federal Information Resources, Transmittal 4," November 30, 2000
- (k) DoD Directive 5000.1, "The Defense Acquisition System," *May 12, 2003*
- (l) Sections 1423 and 1451 of title 40, United States Code, "Division E of the Clinger-Cohen Act of 1996"
- (m) DoD Directive O-8530.1, "Computer Network Defense," January 8, 2001
- (n) DoD 5200.2-R, "DoD Personnel Security Program," *December 16, 1986*
- (o) DoD 5200.1-R, "DoD Information Security Program Regulation," January 14, 1997
- (p) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
- (q) DoD Directive 5230.20E, "Visits *and* Assignments of Foreign Nationals," *June 22, 2005*
- (r) DoD Instruction 5230.27, "Presentation of DoD-Related Scientific and Technical Papers at Meetings," October 6, 1987
- (s) DoD Directive 5230.9, "Clearance of DoD Information for Public Release," April 9, 1996
- (t) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 6, 1999
- (u) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP)," December 30, 1997
- (v) DoD Directive C-5200.5, "Communications Security (COMSEC)," (U) April 21, 1990
- (w) National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-enabled Information Technology Products," January 2000
- (x) DoD Directive *3020.40, "Defense Critical Infrastructure Program (DCIP)," August 19, 2005*
- (y) DoD 5220.22-M, "National Industrial Security Program Operating Manual," January 1995 and "National Industrial Security Program Operating Manual Supplement," February 1995

² Available at <http://www.nstissc.gov/html/library.html>

- (z) Title 48, Code of Federal Regulations, "Federal Acquisition Regulations System," October 1, 1996³
- (a) Information Assurance Technical Framework (IATF), Release 3.0, September 2000⁴
- (a) DoD 7000.14-R, Vol 2B, Chapter 5, "DoD Financial Management Regulation," June 2000
- (a) Section 552a of title 5, United States Code, "The Privacy Act of 1974"
- (a) Section 278g-3 of title 15, United States Code, "Computer Security Act of 1987"
- (a) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998
- (a) Section 552 of title 5, United States Code, "Freedom of Information Act"
- (a) DoD Directive 5210.83, "Department of Defense Unclassified Controlled Nuclear Information (DoD UCNI)", November 15, 1991
- (a) DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984

³ Available at <http://web1.deskbook.osd.mil/htmlfiles/rlcats.asp>

⁴ Available at <http://www.iatf.net>

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Application. Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring or administrative privileges. Examples include office automation, electronic mail, web services, and major functional or mission software programs.

E2.1.2. Authentication. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information (reference (i)).

E2.1.3. Authorized User. Any appropriately cleared individual with a requirement to access a DoD information system in order to perform or assist in a lawful and authorized governmental function.

E2.1.4. Availability. Timely, reliable access to data and information services for authorized users (reference (i)).

E2.1.5. Community Risk. Probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population.

E2.1.6. Computer Network. The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities such as local or campus area networks, or long-haul data transport capabilities such as operational, metropolitan, or wide area and backbone networks.

E2.1.7. Computing Environment. Workstation or server (host) and its operating system, peripherals, and applications (reference (i)).

E2.1.8. Confidentiality. Assurance that information is not disclosed to unauthorized entities or processes (reference (i)).

E2.1.9. Connection Approval. Formal authorization to interconnect information systems.

E2.1.10. Controlled Unclassified Information. A term used, but not specifically defined in reference (o), to refer to sensitive information as defined in paragraph E2.1.41., below.

E2.1.11. Defense-in-Depth. The DoD approach for establishing an adequate IA posture in a shared-risk environment that allows for shared mitigation through: the integration of people, technology, and operations; the layering of IA solutions within and among IT assets; and, the selection of IA solutions based on their relative level of robustness.

E2.1.12. Defense Information System Network (DISN). The DoD consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations.

E2.1.13. Designated Approving Authority (DAA). The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority (reference (i)).

E2.1.14. DISN Designated Approving Authority (DISN DAA). One of four DAAs responsible for operating the DISN at an acceptable level of risk. The four DISN DAAs are the Directors of the DISA, the DIA, the NSA and the Director of the Joint Staff (delegated to the Joint Staff Director for Command, Control, Communications, and Computer Systems (J-6)).

E2.1.15. DMZ (Demilitarized Zone). Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's IA policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal network from outside attacks. A DMZ is also called a "screened subnet."

E2.1.16. DoD Information System. Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections.

E2.1.16.1. Automated Information System (AIS) Application. For DoD information assurance purposes, an AIS application is the product or deliverable of an acquisition program, such as those described in reference (k). An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support); multiple software applications that are related to a single mission (e.g., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System, Defense

Messaging System). AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave. Note that an AIS application is analogous to a "major application" as defined in reference (j); however, this term is not used in order to avoid confusion with the DoD acquisition category of Major Automated Information System.

E2.1.16.2. Enclave. Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems as defined in reference (j). Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

E2.1.16.3. Outsourced IT-based Process. For DoD IA purposes, an outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.

E2.1.16.4. Platform IT Interconnection. For DoD IA purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition, and operations. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric. Examples of platform IT interconnections that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration.

E2.1.17. Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

E2.1.18. IA Certification and Accreditation. The standard DoD approach for identifying information security requirements, providing security solutions, and managing the security of DoD information systems.

E2.1.19. IA Control. An objective IA condition of integrity, availability or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format, i.e., a control number, a control name, control text, and a control class. Specific management, personnel, operational, and technical controls are applied to each DoD information system to achieve an appropriate level of integrity, availability, and confidentiality in accordance with reference (j).

E2.1.20. IA Product. Product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control, non-repudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls, and intrusion detection devices.

E2.1.21. IA-Enabled Information Technology Product. Product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems.

E2.1.22. Information Owner. Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

E2.1.23. Integrity. Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information (reference (i)).

E2.1.24. IT Position Category. Applicable to unclassified DoD information systems, a designator that indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. Position categories include: IT-I (Privileged), IT-II (Limited Privileged) and IT-III (Non-Privileged), as defined in reference (o). Investigative requirements for each category vary, depending on role and whether the incumbent is a U.S. military member, U.S. civilian government employee, U.S. civilian contractor or a foreign national. The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position.

E2.1.25. Mission Assurance Category (MAC). Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories:

E2.1.25.1. Mission Assurance Category I (MAC I). Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

E2.1.25.2. Mission Assurance Category II (MAC II). Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure adequate assurance.

E2.1.25.3. Mission Assurance Category III (MAC III). Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.

E2.1.26. Mobile Code. Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient.

E2.1.27. National Information Assurance Partnership (NIAP). Joint initiative between the NSA and the National Institute of Standards and Technology responsible for security testing needs of both IT consumers and producers and promoting the development of technically sound security requirements for IT products and systems and appropriate measures for evaluating those products and systems.

E2.1.28. Need-to-Know. Necessity for access to, or knowledge or possession of, specific official DoD information required to carry out official duties (reference (i) modified).

E2.1.29. Need-to-Know Determination. Decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties (reference (i)).

E2.1.30. Non-repudiation. Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data (reference (i)).

E2.1.31. Official DoD Information. All information that is in the custody and control of the Department of Defense, relates to information in the custody and control of the Department, or was acquired by DoD employees as part of their official duties or because of their official status within the Department (reference (s)).

E2.1.32. Portfolio. The aggregate of IT investments for DoD information systems, infrastructure and related technical activities that are linked to mission goals, strategies, and architectures, using various assessment and analysis tools to permit information and IT decisions to be based on their contribution to the effectiveness and efficiency of military missions and supporting business functions. Portfolios enable the Department of Defense to manage IT resources and align strategies and programs with Defense-wide, functional, and organizational goals and measures.

E2.1.33. Proxy. Software agent that performs a function or operation on behalf of another application or system while hiding the details involved. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client network address is authorized to use the requested service, optionally perform additional authentication, and then complete a connection on behalf of the user to a remote destination.

E2.1.34. Public Domain Software. Software not protected by copyright laws of any nation that carries no warranties or liabilities, and may be freely used without permission of or payment to the creator.

E2.1.35. Public Information. Official DoD information that has been reviewed and approved for public release by the information owner in accordance with reference (s).

E2.1.36. Research and Technology. Activities that may be described as basic research, applied research, and advanced technology development, demonstrations or equivalent activities, regardless of budget activity. Definitions for Basic Research, Applied Research and Advanced Technology Development are provided in the DoD FMR, Chapter 5 (reference (a^h)).

E2.1.37. Robustness. A characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly. The Department of Defense has three levels of robustness:

E2.1.37.1. High Robustness: Security services and mechanisms that provide the most stringent protection and rigorous security countermeasures.

E2.1.37.2. Medium Robustness: Security services and mechanisms that provide for layering of additional safeguards above good commercial practices.

E2.1.37.3. Basic Robustness: Security services and mechanisms that equate to good commercial practices.

E2.1.38. Security Domain. Within an information system, the set of objects that is accessible. Access is determined by the controls associated with information properties such as its security classification, security compartment or sensitivity. The controls are applied both within the information system and in its connection to other classified or unclassified information systems.

E2.1.39. Sensitive But Unclassified (SBU). A term commonly and inappropriately used within the Department of Defense as a synonym for Sensitive Information, which is the preferred term.

E2.1.40. Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

E2.1.41. Sensitive Information. Information the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of title 5, United States Code, "The Privacy Act" (reference (a)), but which has not been specifically authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (Section 278g-3 of title 15, United States Code, "The Computer Security Act of 1987" (reference (a))).) This includes information in routine DoD payroll, finance, logistics, and personnel management systems. Sensitive information sub-categories include, but are not limited to the following:

E2.1.41.1. For Official Use Only (FOUO). In accordance with DoD 5400.7-R (reference (a)), DoD information exempted from mandatory public disclosure under the Freedom of Information Act (FOIA) (reference (a)).

E2.1.41.2. Privacy Data. Any record that is contained in a system of records, as defined in the reference (a) and information the disclosure of which would constitute an unwarranted invasion of personal privacy.

E2.1.41.3. DoD Unclassified Controlled Nuclear Information (DoD UCNI). Unclassified information on security measures (security plans, procedures and equipment) for the physical protection of DoD Special Nuclear Material (SNM), equipment, or facilities in accordance with DoD Directive 5210.83 (reference (a₅)). Information is Designated DoD UCNI when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, equipment, or facilities.

E2.1.41.4. Unclassified Technical Data. Data that is not classified, but is subject to export control and is withheld from public disclosure according to DoD Directive 5230.25 (reference (a₁)).

E2.1.41.5. Proprietary. Information that is provided by a source or sources under the condition that it not be released to other sources.

E2.1.41.6. Foreign Government Information. Information that originated from a foreign government and that is not classified CONFIDENTIAL or higher, but must be protected in accordance with reference (o).

E2.1.41.7. Department of State Sensitive But Unclassified (DoS SBU). Information which originated from the DoS that has been determined to be SBU under appropriate DoS information security policies.

• E2.1.41.8. Drug Enforcement Administration (DEA) Sensitive Information. Information originated by the DEA that requires protection against unauthorized disclosure to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports.

E2.1.42. Supporting IA Infrastructures. Collections of interrelated processes, systems, and networks that provide a continual flow of information assurance services throughout the Department of Defense, e.g., the key management infrastructure or the incident detection and response infrastructure.

E2.1.43. Telework. Any arrangement in which an employee performs officially assigned duties at an alternative worksite on either a regular and recurring, or on an ad hoc, basis (not including while on official travel).

Input from Dean David Nicol

In its relatively short lifespan, the Information Security & Intelligence (ISI) program has risen to a point of prominence. The program, through the exceptional efforts of its faculty, has attained regional and national recognition for its curricular content; secured a substantial NSF grant to support research; initiated external linkages, from regional to international; and grown enrollment at a prodigious rate.

The ISI program provides its students with knowledge and skill development that has been confirmed externally as consistent with the current needs of both the public and private sectors. Our extremely talented faculty (reflecting academic training and industry experience) are constantly assessing our offerings to assure currency and relevance. The dynamic curriculum has already incorporated curricular changes prompted by feedback from our multiple constituencies. Of course, as noted in the report, sustainability of this program necessitates our continuing attention in this regard, both in terms of internal assessment, and environmental scanning.

In addition to the dynamic nature of the curriculum, the program locus, with its significant emphasis on remote delivery, represents both an opportunity and a challenge. Again, as noted, the enrollment growth, spread across an expanding number of locations and delivery modes, renders it infeasible to provide necessary coverage by permanent faculty. Hence, it is critical that we identify qualified adjunct faculty, and ensure monitoring/mentoring by our permanent faculty to assure the continuing distinctive quality of our program.

The need to effectively utilize adjunct faculty is also prompted by the numerous, but related, academic directions in which the program faculty is engaged: taking the ISI curriculum to the graduate level; supporting curricular offshoots (e.g., Project Management); exploring international linkages; and, engaging in more extensive research activities. We are fortunate to have an exceptional cadre of faculty associated with this program, but it is critical that we engage in resource planning so that we avoid faculty burnout and ensure that all that we undertake is attended to appropriately.

As noted as well, it is critical that we attend to how to more effectively connect with prospective students. In an increasingly competitive environment, we cannot assume students will find their way to us; we have to target them, and do so in a manner that is convincing. We have a distinctive and valuable offering. The challenge is to make the right segment of the prospective student population aware, and that they are compelled to act on that awareness.