

**Information Assurance Concentration**  
**In the Master of Management Information Systems (MIS)**

**At**

**The University of Nebraska at Omaha**

**By**

**Dwight A. Haworth, Ph.D.**  
**Leah R. Pietron, Ph.D.**

**Associate Professors**  
**Department of Information Systems/  
Quantitative Analysis (ISQA)**

**Blaine W. Burnham, Ph.D.**

**Director,**  
**Nebraska University**  
**Center of Information Assurance (NUCIA)**

**Track:**

**Integrating information assurance topics in existing graduate or undergraduate  
curricula**

## **Abstract**

The growth and availability of the Internet created serious vulnerabilities in connected systems. In response to this, the Federal Government has created several programs. Significant among those is the National Security Telecommunications and Information Systems Security Policy and the implementing directives that specify training standards for various professional positions related to telecommunications and information systems security.

In response to the directives of the National Security Telecommunications and Information Systems Security Committee (NSTISSC) and to the results of independent research, the faculty of the College of Information Science and Technology at the University of Nebraska at Omaha decided to implement a concentration in Information Assurance as an option in the Master of Science in Management Information Systems Program. To cover the subject matter indicated by NSTISSC directives and by security incidents described in the press, four courses have been established and a fifth is in preparation: ISQA 8530 — Electronic Commerce Security, ISQA 8540 — Computer Security Management, ISQA 8560 — Information Warfare and Security, ISQA 8570 — Information Security Policy, Privacy, and Ethics, and ISQA 8580 — Computer Security Investigations (under development).

After developing these courses, an additional measure was undertaken to determine the coverage of the NSTISSC standards in these four courses. A spreadsheet was created to reflect the content coverage of the NSTISSC standards. The study determined the courses of the Information Assurance concentration provide substantial coverage of the requirements of NSTISSI No. 4013 - National Training Standard for System Administration in Information Systems Security. There is also coverage of topics relevant to the needs of the business community. The items of NSTISSI No. 4013 that are not covered are those peculiar to

government operations and the evaluation scenario posited by that Standard. Based on these results, it is concluded that the courses of the Information Assurance concentration provide background and preparation for students to enter the field of Information Assurance in either business or government service.

## **I. Introduction**

In the early 1990s, several government agencies recognized a need to address the vulnerabilities created in the new information age. Several forms of legislation were implemented to create three very important organizations/commissions/programs: NSTISSC (National Security Telecommunications and Information Systems Security), PCCIP (President's Commission on Critical Infrastructure Protection), and Federal Cyber Service: Scholarship for Service (SFS).

In July 1996, by Presidential Executive Order 13010, the PCCIP (President's Commission on Critical Infrastructure Protection) was created. This commission was tasked to formulate a comprehensive national strategy for protecting the infrastructures we all depend on from physical and "cyber" threats [1]. The PCCIP advises and assists the President of the United States by recommending a national strategy for protecting and assuring critical infrastructures from physical and cyber threats. The Commission identified eight critical infrastructures: telecommunications, electrical power systems, gas and oil, banking and finance, transportation, water supply systems, government services and emergency services. [2].

The National Security Telecommunications and Information Systems Security Committee (NSTISSC) was established by National Security Directive 42 (NSD-42) and issued on July 5, 1990 [3]. The NSTISSC provides a forum for discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of national security systems through the NSTISSC Issuance System. [4]

One of the primary functions of NSTISSC is to develop and issue national policy and standards. Among the current NTISS/NSTISS Standards being incorporated into educational programs are:

NSTISSI No. 4011 - National Training Standard for Information Systems Security (INFOSEC) Professionals, June 20,1994

NSTISSI No. 4012 - National Training Standard for Designated Approving Authority (DAA), August 1997

NSTISSI No. 4013 - National Training Standard for System Administration in Information Systems Security, August 1997

NSTISSI No. 4014 - National Training Standard for Information Systems Security Officers (ISSO), August 1997

NSTISSI No. 4015 - National Training Standard for Systems Certifiers, dated December 2000 [5]

Another key program developed was the Federal Cyber Service. This program seeks to increase the number of qualified students entering the fields of information assurance and computer security and to increase the capacity of the United States higher education enterprise to continue to produce professionals in these fields [6]. The program has three tracks:

Scholarship Track Scholarship - recipients will become part of the Federal Cyber Service of Government's information infrastructure. After their two-year scholarships, the recipients will be required to work for a federal agency for two years as their Federal Cyber Service commitment.

Faculty Development Track - provides funds for institutions with Center of Academic Excellence in Information Assurance Education (CAE/IAE) certification, or equivalent institutions, to conduct regional and national faculty development seminars for faculty teams from non-CAE/IAE institutions.

Institutional Development Track - provides funds for institutions not currently eligible for the Scholarship Track to develop institutional capacity in the information assurance and computer security area [6]

After reviewing these policies and programs, there remained a need to determine the demand that could be expected from the business community. To estimate the demand, a

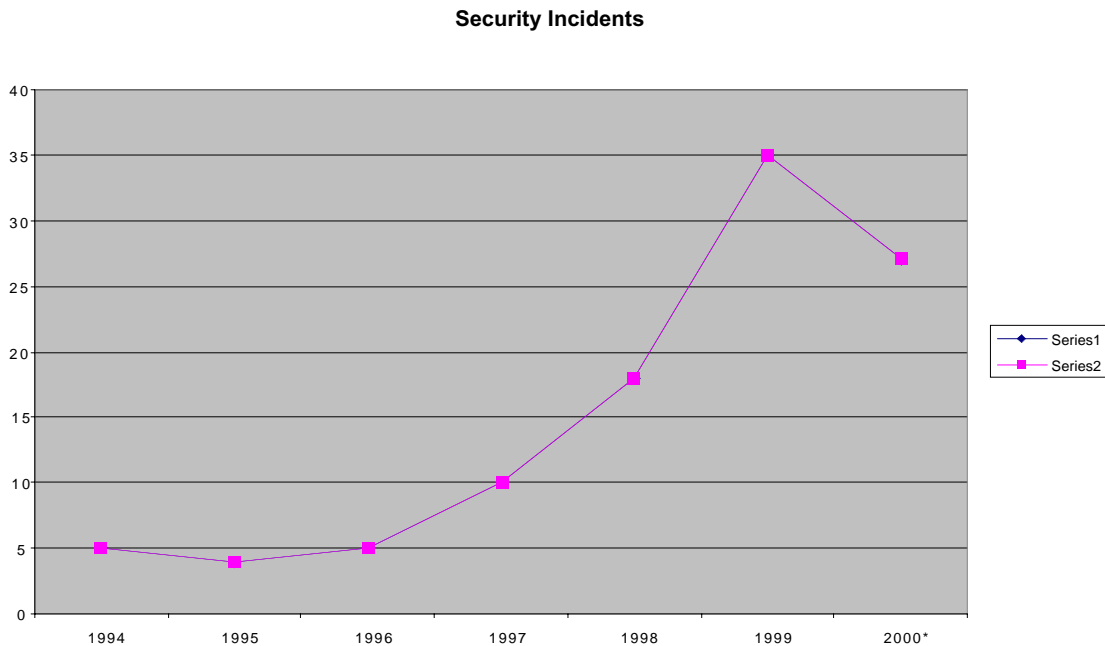
research study was conducted to determine the numbers and types of security incidents being experienced by businesses and government agencies.

### **A. Research Study on Security Incidents**

Over the next six months, a log was created that recorded the reports of security incidents in the trade press, specifically ComputerWorld. ComputerWorld was selected as an available and representative member of the computer trade press, one that reflected significant events as well as the concerns of the computer community. Further, to the extent that the press can focus opinion, it was felt that through its reporting ComputerWorld could influence which issues would become major concerns of the computer community in the future.

The log included not only new reports recorded from current issues but also entries developed from the archives of ComputerWorld. ComputerWorld's searchable database of reports was examined for all security incidents over six years, up to October of 2000. The result was a small database with 105 entries. These entries covered the spectrum of computer security incidents, from e-mail floods to Trojan attacks, from outright intrusions to distributed denial of service incidents. The result parallels reports from other sources, namely that the number of security incidents seems to be increasing.

The graph clearly shows a dramatic increase in the number of security incidents reported in the press. The data for 2000 is incomplete, but it appears that it will match the number posted in 1999. Clearly, security is a concern. Moreover, the trend suggests that the future will demand a better understanding of security issues and practices from students who complete formal programs of education and that there will be a market for those who specialize in information assurance.



To determine the thrust of our effort to satisfy the expected demand, we reviewed the programs being offered in our region. Currently, NSTISS Instructions Nos. 4011, 4012, & 4015 are being incorporated into the University of Tulsa Computer Science graduate program [7]. When reviewing our current graduate program, it was determined that several of the proposed courses in the Information Assurance concentration for Master of Science in MIS would satisfy most or all of the requirements for NSTISSI No. 4013, National Training Standard for System Administration in Information Systems Security. The following narrative explains the core content of the MS in MIS program, the concentrations in E-Commerce and Information Assurance.

## **II. Master in Management Information Systems (MIS)**

The existing Master of Science in Management Information Systems was selected as a starting point. The prescribed coursework consists of eight required courses, which are described below, and four elective courses. The program had been designed to encourage

students to use the elective courses to create a concentration in a specialty area, and courses exist that allow the student to build a concentration in Electronic Commerce. The coursework of the Master of Science in Management Information Systems and Electronic Commerce concentration courses follow.

**ISQA 8060 - Research in Management Information Systems**

This course covers research methods and their application to the development and evaluation of management information systems. Also covered is the relationship between organization theory and IS research. Students design a research study for an organization and apply the research techniques for the analysis of the project. A sampling of topics covered include: types of research, nature of measurement, information systems measures overview, reasons for measurement, measurement of human behavior, and characteristics of scientific research.

**ISQA 8110 - Modern Software Design**

This course gives the student an understanding of object-oriented software design. The student will understand the relationships between structured programming, data hiding, data abstraction, and object oriented programming. The student will understand the effect of program design attributes on the maintainability of a program. Finally, the student will apply an object-oriented analysis and design methodology to complete a major assignment.

**ISQA 8210 - Management of Software Development**

This course covers concepts and techniques from software engineering, management science, psychology, organization behavior, and organization change to identify, understand, and propose solutions to the problems of software project management. The purpose of the course is to prepare the student for leadership positions in software development and software maintenance. Additional topics include: software process maturity, waterfall and spiral process model, prototyping process model, PERT, function point estimation, and change management and design.

**ISQA 8220 - Systems Analysis and Design**

This course covers advanced systems analysis and design techniques. Emphasis will be placed on both the object-oriented and the structured approaches to systems analysis and design. A variety of life cycle models such as the Waterfall model, Rapid Prototyping Model, the Incremental Model, the Spiral Model and Foundation model are presented, compared, and contrasted. The IEEE standards for performance of analysis and design activities are presented and discussed. All projects must be based on a software development standard such as the IEEE standards, the Department of Defense Standards, or ISO Standards or a combination of these standards.

### **ISQA 8310 - Data Communications**

This course provides a comprehensive review of data and computer communications for business information systems within the framework of the ISO OSI model, evolving techniques for effective data communications, telecommunications infrastructure and services, and the design and management of organizational data and voice communications resources. This class maintains strong emphasis on the business and managerial perspective on the technology. Additional topics include: communications architecture, local area networks, wide area networks, high-speed networking, internetworking, computer/telephony integration, networking management and security, and TCP/IP.

### **ISQA 4380/8386 - Managing the Client/Server Environment**

The course gives students a grounding in the concepts, issues, and tools needed to manage client/server environments. It focuses on client/server technologies, the issues faced in building and managing client/server systems, and the strategic relationship between business process and the information systems architecture. Students will build a client/server system. Additional topics include: middleware, distributed data systems, standards, distributed object-oriented computing, the internet and client/server computing, enterprise application integration, client/server systems performance, and enterprise systems management.

### **ISQA 8410 - Database Management**

The course has a two pronged focus: the role of the data administrator and the relational database model. Focus on the foundations, issues, costs, benefits, and problem areas of database and database administration. The course will emphasize strategic planning, modeling, and administration of a database environment. Current database management systems (DBMS) software will be used to supplement the course. A sample of the course topics include: the relational model, data definition language, data manipulation language, data control language, entity-relationship diagramming, logical and physical database design, data and database administration, and data warehousing.

### **ISQA 8810 - IT Project Fundamentals**

The course will integrate concepts and techniques from management science, psychology, organizational behavior, and administration change to identify, understand, and propose solutions to the problems of project management. The purpose of the course is to prepare the graduate for project participation and leadership. A sample of course topics include: fundamentals and the issue of project scope, project time, project cost, project quality, communications, procurement, human resources, and risk management.

[8]

## **A. MS IN MIS - E-COMMERCE CONCENTRATION**

MIS program may now opt to take a concentration in electronic commerce. A concentration will appear on your transcript. The e-commerce concentration consists of four

courses, one required course and three electives to be picked from the list below. Additional electives may be added to this list in the future.

- ISQA 8186 - Electronic Commerce (required)
- ISQA 8196 - Process Re-engineering with IT (elective)
- ISQA 8525 - Graphical User Interface Design (elective)
- ISQA 8700 - Data Warehousing: Theory and Practice (elective)
- ISQA 8080 - Seminar in MIS (elective - the seminar topic MUST be related to e-commerce.)

## **B. MS IN MIS — PROPOSED INFORMATION ASSURANCE CONCENTRATION**

It was felt that an offering of four or five elective courses would allow the student to form a strong Information Assurance concentration. In addition, there was a motivation to create courses that would be complementary to and accepted in the existing program and that would spread awareness and understanding to students outside the Information Assurance field.

Five courses were developed for the concentration in Information Assurance. The courses are listed below and four brief course outlines follow:

- ISQA 8530 — Electronic Commerce Security
- ISQA 8540 — Computer Security Management
- ISQA 8560 — Information Warfare and Security
- ISQA 8570 — Information Security Policy, Privacy, and Ethics
- ISQA 8580 — Computer Security Investigations (under development)

### **ISQA 8530 E-COMMERCE SECURITY**

#### **COURSE DESCRIPTION**

##### Overview of content and purpose of the course

The course will integrate concepts, principles and technologies from business, telecommunications, and computer science to identify, understand, and propose solutions to the security threats to e-commerce. The purpose of this course is to prepare the student to specify and select security alternatives for e-commerce sites.

#### **CONTENT AND ORGANIZATION**

##### List of topics to be covered in chronological sequence

1. The scope and nature of e-commerce,
2. Security threats to e-commerce,

3. Fundamentals of the Internet,
4. Legal aspects of commerce,
5. Information security technologies,
6. Personnel vulnerabilities,
7. Security aspects of the Internet,
8. Client-side vulnerabilities,
9. Transmission vulnerabilities,
10. Server-side vulnerabilities,
11. Operating system vulnerabilities,
12. Certificates,
13. Public-key infrastructures,
14. Non-repudiation,
15. Certification practices.

**ISQA 8540**  
**COMPUTER SECURITY MANAGEMENT**

**COURSE DESCRIPTION**

Overview of content and purpose of the course

The course will integrate concepts and techniques from management, computer science, and organizational behavior to identify, understand, and propose solutions to the problems of computer security and security administration. The purpose of the course is to prepare the student for leadership positions in computer system management.

**CONTENT AND ORGANIZATION**

List of topics to be covered in chronological sequence

1. Overview of Computer Security,
2. Physical Protection,
3. Hardware Security Controls,
4. Software Controls,
5. Configuration Management,
6. Encryption Techniques,
7. Database Security,
8. Telecommunications Security,
9. Microcomputer Security,
10. Viruses
11. Legal Issues
12. Current Legislation
13. Ethical Use of Computers
14. Security Policy and Managerial Issues
15. Disaster Planning and Recovery
16. New Technologies and Trends

**ISQA 8560**  
**INFORMATION WARFARE AND SECURITY**

**COURSE DESCRIPTION**

Overview of content and purpose of the course

This course will study the nature of information warfare, including computer crime and information terrorism, as it relates to international, national, economic, organizational, and personal security. Information warfare policy and ethical issues will be examined.

**CONTENT AND ORGANIZATION**

List of topics to be covered in chronological sequence

1. Overview of Information Warfare (IW)
2. Information Warfare in Context
3. Export Controls on Cryptography
4. Open Sources, Psyops and Perception Management
5. Insider Threat, Espionage
6. Signals Intelligence, Fraud, and Sabotage
7. Computer Break-ins, Hacking, Masquerading, Cyberplagues
8. Secrecy and Authentication
9. Monitors, Gatekeepers, Risk Management, Incident Handling
10. The IW Threat
11. Defensive IW Policy and Programs
12. Encryption Policy
13. IW Policy and Ethics

**ISQA 8570**  
**INFORMATION SECURITY POLICY, PRIVACY, AND ETHICS**

**COURSE DESCRIPTION**

Overview of content and purpose of the course

The course will cover the development and need for information security policies, issues regarding privacy, and the application of computer ethics.

**CONTENT AND ORGANIZATION**

List of topics to be covered in chronological sequence

1. The Need for Security
2. The Importance of a Security Policy
3. Building a Foundation for the Policy
4. Analyzing Risks
5. Developing a Security Policy
6. Communicating Policy to Users
7. Implementing the Policy
8. The Problem with Content
9. The Problem with Privacy

10. Copyrights, Freedom of Speech, and Related Rights
11. Trademarks and Unfair Competition in Cyberspace
12. Patents, Trade Secrets, Antitrust, and Standards
13. Protecting Consumers and Their Privacy: Tools and Agents
14. Intellectual Property
15. Use of Computer Services
16. Privacy Rights
17. Ownership of Programs
18. Proprietary Resources

### **III. Conclusion**

To evaluate the content of the courses and determine the thoroughness of the coverage, we constructed a spreadsheet of Appendix I of NSTISSI No. 4013 - National Training Standard for System Administration in Information Systems Security. The items of Appendix I were listed in the rows of the spreadsheet and the courses were listed as columns. When an individual item was addressed in a course, a 1 was placed in the row of the item and under the column of the course. The faculty members responsible for each course were asked to fill out the column for each course as they now teach it. An item of question was the exact meaning of the terms used in the Standard, for example, does "define" mean to specify and promulgate a listed item or does it mean to outline the essential elements of a listed item. It was felt that our students should be able to perform the latter, but that they would have no experience in actually writing and promulgating a policy or procedure. Pending resolution of this ambiguity, the faculty were directed to interpret these items conservatively. A column was inserted in which row summations could be calculated; a 0 would indicate no coverage and any positive number would indicate coverage of the item. The resulting spreadsheet is included as Appendix I.

We conclude that the courses of the Information Assurance concentration provide substantial coverage of the requirements of NSTISSI No. 4013 - National Training Standard for System Administration in Information Systems Security. Most of the items that are not covered

are those peculiar to government operations and the evaluation scenario of the Standard. The spreadsheet does spotlight items that deserve further attention:

- 1) the need for a "local" environment in which students can put into practice many of the elements of the Standard, and
- 2) the lack of coverage of TEMPEST.

Some of the former may be covered in classroom or laboratory exercises after appropriate exercise material has been prepared. Coverage of TEMPEST materials may require outside assistance, such as USSTRATCOM.

This study demonstrates that the courses of the Information Assurance concentration provide substantial coverage of the requirements of NSTISSI No. 4013 - National Training Standard for System Administration in Information Systems Security. There is also coverage of topics relevant to the needs of the business community. The items of NSTISSI No. 4013 that are not covered are those peculiar to government operations and the evaluation scenario posited by that Standard. Based on these results, it is concluded that the courses of the Information Assurance concentration provide background and preparation for students to enter the field of Information Assurance in either business or government service.

Clearly, the construction of the spreadsheet has a two-fold benefit. It allows us to perform an evaluation of our current program, and it will support future improvements and ongoing evaluation.

#### **IV. Bibliography**

- [1] President's Commission on Critical Infrastructure Protection, Executive Order 13010 [Online]. Available: <http://www.info-sec.com/pccip/web/eo13010.html>
- [2] Fact Sheet President's Commission on Critical Infrastructure Protection. [Online]. Available: <http://www.info-sec.com/pccip/web/backgrd.html> -
- [3] The National Security Telecommunications and Information Systems Security Committee (NSTISSC). [Online]. Available: <http://www.nstissc.gov/html/overview.html>
- [4] The National Security Telecommunications and Information Systems Security Committee (NSTISSC), Functions. [Online]. Available: <http://www.nstissc.gov/html/functions.html>
- [5] NSTISSC Library Files. [Online]. Available: <http://www.nstissc.gov/html/library.html>
- [6] Federal Cyber Service: Scholarship for Service (SFS). [Online]. Available: <http://www.ehr.nsf.gov/ehr/duo/programs/sfs/>
- [7] Computer Science Program - University of Tulsa. [Online]. Available: <http://www.mcs.utulsa.edu/grad.cs.courses.html>
- [8] University of Nebraska at Omaha, Department of Information Systems/Quantitative Analysis, Master of Science in Management Information Systems. [Online]. Available: <http://www.isqa.unomaha.edu/gpgm.htm>

## V. Appendix Coverage of Security Standards

|   | ISQA<br>Coverage | ISQA<br>8530 | ISQA<br>8540 | ISQA<br>8560 | ISQA<br>8570 |
|---|------------------|--------------|--------------|--------------|--------------|
| <b>1. GENERAL</b>   |                  |              |              |              |              |
| <b>a. Security Policy</b>   |                  |              |              |              |              |
| (1) define local accountability policies;                                       | 1                |              |              |              | 1            |
| (2) explain accreditation;  | 0                |              |              |              |              |
| (3) discuss three agency specific security policies;                            | 0                |              |              |              |              |
| (4) define assurance;   | 1                |              | 1            |              |              |
| (5) explain certification policies as related to local requirements;            | 1                |              |              |              | 1            |
| (6) define local e-mail privacy policies;                                       | 1                |              |              |              | 1            |
| (7) describe local security policies relative to electronic records management; | 0                |              |              |              |              |
| (8) explain security policies relating to ethics;                               | 1                |              |              |              | 1            |
| (9) describe relevant FAX security policies;                                    | 1                |              |              |              | 1            |
| (10) discuss the concept of information confidentiality;                        | 4                | 1            | 1            | 1            | 1            |
| (11) identify information ownership of data held under his/her cognizance;      | 0                |              |              |              |              |
| (12) identify information resource owner/custodian;                             | 2                |              | 1            |              | 1            |
| (13) define local information security policy;                                  | 1                |              |              |              | 1            |
| (14) describe information sensitivity in relation to local policies;            | 1                |              |              | 1            |              |
| (15) discuss integrity concepts;  | 4                | 1            | 1            | 1            | 1            |
| (16) describe local policies relevant to Internet security;                     | 0                |              |              |              |              |
| (17) explain local area network (LAN) security as related to local policies;    | 2                |              | 1            |              | 1            |
| (18) define policies relating to marking of sensitive information;              | 1                |              |              | 1            |              |
| (19) understands fundamental concepts of multilevel security;                   | 3                |              | 1            | 1            | 1            |
| (20) describe policies relevant to network security;                            | 1                |              |              |              | 1            |
| (21) define the functional requirements for operating system integrity;         | 1                |              | 1            |              |              |
| (22) perform operations security (OPSEC) in conformance with local policies;    | 0                |              |              |              |              |
| (23) explain physical security policies;  | 2                |              | 1            |              | 1            |
| (24) discuss local policies relating to secure systems operations;              | 0                |              |              |              |              |
| (25) identify appropriate security architecture for use in assigned IS(s);      | 0                |              |              |              |              |
| (26) describe security domains as applicable to local policies;                 | 1                |              |              |              | 1            |
| (27) define local policies relating to separation of duties;                    | 1                |              |              |              | 1            |
| (28) identify systems security standards policies;                              | 1                |              |              |              | 1            |
| (29) identify the Orange Book;  | 2                |              | 1            |              | 1            |
| (30) identify TEMPEST policies;   | 0                |              |              |              |              |
| (31) define TEMPEST policies;   | 0                |              |              |              |              |
| (32) define validation and testing policies;                                    | 2                |              | 1            |              | 1            |
| (33) identify verification and validation process policies;                     | 0                |              |              |              |              |
| (34) define verification and validation process policies;                       | 1                |              |              |              | 1            |
| (35) describe wide area network (WAN) security policies;                        | 0                |              |              |              |              |
| (36) use/implement WAN security policies;                                       | 0                |              |              |              |              |
| (37) describe workstation security policies;                                    | 2                |              | 1            |              | 1            |
| (38) use/implement workstation security policies; and                           | 0                |              |              |              |              |
| (39) describe zoning and zone of control policies.                              | 0                |              |              |              |              |

## **b. Procedures**

|   |   |   |   |   |
|---|---|---|---|---|
| (1) practice/use facility management procedures;            | 0 |   |   |   |
| (2) describe FAX security procedures;                       | 2 | 1 |   | 1 |
| (3) practice/use FAX security procedures;                   | 0 |   |   |   |
| (4) describe housekeeping procedures;                       | 2 | 1 |   | 1 |
| (5) perform housekeeping procedures;                        | 0 |   |   |   |
| (6) describe information states procedures;                 | 2 | 1 |   | 1 |
| (7) distinguish among information states procedures;        | 0 |   |   |   |
| (8) explain Internet security procedures;                   | 3 | 1 | 1 | 1 |
| (9) use Internet security procedures;                       | 0 |   |   |   |
| (10) explain marking of sensitive information procedures ** | 0 |   |   |   |
| (11) perform marking of sensitive information procedures ** | 0 |   |   |   |
| (12) apply multilevel security;                             | 2 |   | 1 | 1 |
| (13) explain the principles of network security procedures; | 3 | 1 |   | 1 |
| (14) use network security procedures;                       | 0 |   |   |   |
| (15) describe operating system integrity procedures;        | 1 |   | 1 |   |
| (16) perform operating systems security procedures;         | 0 |   |   |   |
| (17) assist in local security procedures;                   | 0 |   |   |   |
| (18) describe purpose and contents of the Red Book;         | 2 |   | 1 | 1 |
| (19) describes secure systems operations procedures;        | 1 |   | 1 |   |
| (20) define TEMPEST procedures;                             | 0 |   |   |   |
| (21) identify TEMPEST procedures;                           | 0 |   |   |   |
| (22) identify certified TEMPEST technical authority (CTTA); | 0 |   |   |   |
| (23) describe WAN security procedures;                      | 2 |   | 1 | 1 |
| (24) practice WAN security procedures; and                  | 0 |   |   |   |
| (25) explain zoning and zone of control procedures.         | 0 |   |   |   |

## **c. Education, Training, and Awareness**

|  |   |   |   |   |   |
|--|---|---|---|---|---|
| (1) discuss the principle elements of security training;                     | 3 |   | 1 | 1 | 1 |
| (2) explain security training procedures;                                    | 3 |   | 1 | 1 | 1 |
| (3) explain threat in its application to education, training, and awareness; | 3 |   | 1 | 1 | 1 |
| (4) use awareness materials as part of job;                                  | 2 |   |   | 1 | 1 |
| (5) distinguish between education, training, and awareness;                  | 2 |   | 1 |   | 1 |
| (6) give examples of security awareness;                                     | 3 |   | 1 | 1 | 1 |
| (7) give examples of security education;                                     | 3 |   | 1 | 1 | 1 |
| (8) discuss the objectives of security inspections/reviews; and              | 3 |   | 1 | 1 | 1 |
| (9) identify different types of vulnerabilities.                             | 4 | 1 | 1 | 1 | 1 |

## **d. Countermeasures/Safeguards**

|   |   |  |   |   |   |
|---|---|--|---|---|---|
| (1) discuss the different levels of countermeasures/safeguards assurance; | 0 |  |   |   |   |
| (2) describe e-mail privacy countermeasures/safeguards;                   | 2 |  | 1 |   | 1 |
| (3) define Internet security;   | 2 |  | 1 |   | 1 |
| (4) describe what is meant by countermeasures/safeguards;                 | 3 |  | 1 | 1 | 1 |
| (5) describe separation of duties;  | 3 |  | 1 | 1 | 1 |
| (6) define countermeasures/safeguards used to prevent software piracy;    | 1 |  | 1 |   |   |
| (7) define TEMPEST countermeasures/safeguards; and                        | 0 |  |   |   |   |
| (8) explain what is meant by zoning and zone of control.                  | 0 |  |   |   |   |

### **e. Risk Management**

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| (1) explain ways to provide protection for Internet connections;  | 1 | 1 |   |   |   |
| (2) describe operating system integrity;                          | 1 |   | 1 |   |   |
| (3) define TEMPEST as it relates to the risk management process;  | 0 |   |   |   |   |
| (4) identify different types of threat;                           | 4 | 1 | 1 | 1 | 1 |
| (5) explain WAN security; and                                     | 1 |   | 1 |   |   |
| (6) explain what zoning and zone of control ratings are based on. | 0 |   |   |   |   |

## **2. ACCESS CONTROL**

### **a. Policies/Administration**

|  |   |  |   |   |   |
|--|---|--|---|---|---|
| (1) use network access controls as designed;       | 0 |  |   |   |   |
| (2) explain compartmented/partitioned mode;        | 1 |  | 1 |   |   |
| (3) describe data access;                          | 2 |  | 1 |   | 1 |
| (4) identify the dedicated mode of operation;      | 2 |  | 1 |   | 1 |
| (5) explain electronic records management;         | 3 |  | 1 | 1 | 1 |
| (6) define information ownership;                  | 2 |  | 1 |   | 1 |
| (7) identify information resource owner/custodian; | 1 |  | 1 |   |   |
| (8) describe separation of duties; and             | 3 |  | 1 | 1 | 1 |
| (9) define the system high mode.                   | 1 |  | 1 |   |   |

### **b. Countermeasures**

|  |   |   |   |   |   |
|--|---|---|---|---|---|
| (1) describe use of caller ID;               | 1 |   | 1 |   |   |
| (2) give five examples of countermeasures;   | 2 |   | 1 |   | 1 |
| (3) define internal controls and security;   | 3 |   | 1 | 1 | 1 |
| (4) identify methods of intrusion detection; | 3 |   | 1 | 1 | 1 |
| (5) define network firewalls; and            | 4 | 1 | 1 | 1 | 1 |
| (6) describe network security software.      | 4 | 1 | 1 | 1 | 1 |

### **c. Safeguards**

|  |   |   |   |  |   |
|--|---|---|---|--|---|
| (1) demonstrate the ability to use alarms, signals, and reports; | 0 |   |   |  |   |
| (2) identify network security software;                          | 3 | 1 | 1 |  | 1 |
| (3) describe operating system security features;                 | 2 | 1 | 1 |  |   |
| (4) define protected distribution systems; and                   | 1 |   | 1 |  |   |
| (5) describe system security safeguards.                         | 2 |   | 1 |  | 1 |

### **d. Mechanisms**

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| (1) discuss authentication mechanisms;      | 2 | 1 | 1 |   |   |
| (2) describe discretionary access controls; | 2 |   | 1 |   | 1 |
| (3) describe mandatory access controls;     | 2 |   | 1 |   | 1 |
| (4) describe one-time passwords;            | 4 | 1 | 1 | 1 | 1 |
| (5) discuss privileges; and                 | 2 |   | 1 |   | 1 |
| (6) define single sign-on.                  | 2 |   | 1 |   | 1 |

## **3. ADMINISTRATIVE**

### **a. Policies/Procedures**

|   |   |  |   |   |   |
|---|---|--|---|---|---|
| (1) identify basic/generic management issues; | 3 |  | 1 | 1 | 1 |
| (2) define change control policies;           | 2 |  | 1 |   | 1 |

|   |   |   |  |   |
|---|---|---|--|---|
| (3) discuss documentation;                      | 2 | 1 |  | 1 |
| (4) explain electronic records management;      | 2 | 1 |  | 1 |
| (5) describe object reuse;                      | 2 | 1 |  | 1 |
| (6) define operational procedure review;        | 2 | 1 |  | 1 |
| (7) discuss policy enforcement;                 | 2 | 1 |  | 1 |
| (8) identify procedures;                        | 2 | 1 |  | 1 |
| (9) discuss security inspections; and           | 1 | 1 |  |   |
| (10) describe local password management policy. | 1 |   |  | 1 |

#### **b. Countermeasures/Safeguards**

|   |   |   |   |   |
|---|---|---|---|---|
| (1) give examples of alarms, signals and reports;       | 1 | 1 |   |   |
| (2) define application development control;             | 1 | 1 |   |   |
| (3) assist in preparing assessments;                    | 1 |   |   | 1 |
| (4) identify countermeasures;                           | 2 | 1 |   | 1 |
| (5) describe disaster recovery procedures;              | 2 | 1 |   | 1 |
| (6) discuss disposition of classified information;      | 3 | 1 | 1 | 1 |
| (7) practice disposition of media and data;             | 0 |   |   |   |
| (8) practice document labeling;                         | 0 |   |   |   |
| (9) discuss proper use of security safeguards;          | 3 | 1 | 1 | 1 |
| (10) define separation of duties;                       | 3 | 1 | 1 | 1 |
| (11) identify storage media protection and control; and | 0 |   |   |   |
| (12) define system software controls.                   | 2 | 1 |   | 1 |

### **4. AUDIT**

#### **a. Policies/Procedures**

|  |   |   |  |   |
|--|---|---|--|---|
| <b>(1) use alarms, signals and reports in accordance with existing policies and procedures;</b>          | 0 |   |  |   |
| (2) summarize audit-related documentation;   | 0 |   |  |   |
| (3) discuss local policies and procedures for electronic records management; and                         | 1 |   |  | 1 |
| (4) describe three policies and/or procedures in which separation of duties is appropriate or mandatory; | 2 | 1 |  | 1 |

#### **b. Countermeasures/Safeguards**

|   |   |   |  |   |
|---|---|---|--|---|
| (1) identify two countermeasures applicable to audit trail tampering; and | 2 | 1 |  | 1 |
| (2) describe three safeguards gained through use of audit trails.         | 2 | 1 |  | 1 |

#### **c. Tools**

|  |   |   |   |   |
|--|---|---|---|---|
| (1) explain two major benefits of auditing;                          | 2 | 1 |   | 1 |
| (2) identify three audit tools;                                      | 2 | 1 |   | 1 |
| (3) describe the major benefit of audit trails and logging policies; | 2 | 1 |   | 1 |
| (4) define an error log;   | 2 | 1 | 1 |   |
| (5) explain two capabilities offered by expert security/audit tools; | 2 | 1 |   | 1 |
| (6) identify two intrusion detection systems; and                    | 3 | 1 | 1 | 1 |
| (7) describe the major operating system security features.           | 1 | 1 |   |   |

### **5. OPERATIONS**

#### **a. Policies/Procedures**

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| (1) describe disaster recovery policies and procedures;                 | 4 | 1 | 1 | 1 | 1 |
| (2) use/implement disaster recovery policies and procedures;            | 0 |   |   |   |   |
| (3) define disaster recovery policies and procedures;                   | 0 |   |   |   |   |
| (4) describe documentation policy and procedures;                       | 2 |   | 1 |   | 1 |
| (5) use/implement documentation policy and procedures;                  | 0 |   |   |   |   |
| (6) discuss object reuse policy and procedures;                         | 1 |   | 1 |   |   |
| (7) describe separation of duties policies and procedures;              | 2 |   | 1 |   | 1 |
| (8) practice/implement separation of duties policies and procedures;    | 0 |   |   |   |   |
| (9) identify disposition of media and data policies and procedures;     | 0 |   |   |   |   |
| (10) perform disposition of media and data policies and procedures;     | 0 |   |   |   |   |
| (11) explain disposition of media and data policies and procedures; and | 1 |   | 1 |   |   |
| (12) identify storage media protection/control policies and procedures. | 1 |   |   |   | 1 |

**b. Countermeasures/Safeguards**

|   |   |  |   |  |   |
|---|---|--|---|--|---|
| (1) use countermeasure/safeguard alarms, signals and reports;         | 0 |  |   |  |   |
| (2) describe countermeasures;   | 2 |  | 1 |  | 1 |
| (3) use/implement countermeasures/safeguards;                         | 0 |  |   |  |   |
| (4) discuss countermeasure/safeguard corrective actions;              | 2 |  | 1 |  | 1 |
| (5) assist in performing countermeasure/safeguard corrective actions; | 0 |  |   |  |   |
| (6) describe safeguards; and  | 2 |  | 1 |  | 1 |
| (7) use/implement safeguards.   | 0 |  |   |  |   |

**c. Management/Oversight**

|   |   |  |   |  |   |
|---|---|--|---|--|---|
| (1) use/implement management/oversight change controls;   | 0 |  |   |  |   |
| (2) describe configuration management;                    | 1 |  | 1 |  |   |
| (3) discuss database integrity;                           | 1 |  | 1 |  |   |
| (4) describe disaster recovery management/oversight;      | 2 |  | 1 |  | 1 |
| (5) use/implement disaster recovery management/oversight; | 0 |  |   |  |   |
| (6) discuss electronic records management/oversight;      | 2 |  | 1 |  | 1 |
| (7) identify the key elements of information integrity;   | 2 |  | 1 |  | 1 |
| (8) discuss information management;                       | 2 |  | 1 |  | 1 |
| (9) explain risk management; and                          | 1 |  | 1 |  |   |
| (10) practice risk management.                            | 0 |  |   |  |   |

**6. CONTINGENCY**

**a. Continuity of Operations**

|  |   |  |   |  |   |
|--|---|--|---|--|---|
| (1) practice backups;                            | 0 |  |   |  |   |
| (2) describe continuity planning;                | 2 |  | 1 |  | 1 |
| (3) describe disaster recovery;                  | 2 |  | 1 |  | 1 |
| (4) describe disaster recovery plan testing; and | 2 |  | 1 |  | 1 |
| (5) discuss disaster recovery planning.          | 2 |  | 1 |  | 1 |

**b. Countermeasures/Safeguards**

|  |   |  |   |   |   |
|--|---|--|---|---|---|
| (1) use alarms, signals and reports;             | 0 |  |   |   |   |
| (2) define information availability;             | 3 |  | 1 | 1 | 1 |
| (3) identify examples of corrective actions;     | 3 |  | 1 | 1 | 1 |
| (4) select countermeasures;                      | 3 |  | 1 | 1 | 1 |
| (5) identify methods of intrusion detection; and | 3 |  | 1 | 1 | 1 |

|                                    |   |   |   |
|------------------------------------|---|---|---|
| (6) select appropriate safeguards. | 2 | 1 | 1 |
|------------------------------------|---|---|---|

**c. Configuration Management**

|   |   |   |  |
|---|---|---|--|
| (1) practice change controls;                                 | 0 |   |  |
| (2) explain database integrity;                               | 1 | 1 |  |
| (3) practice disposition of classified info;                  | 0 |   |  |
| (4) perform disposition of media and data;                    | 0 |   |  |
| (5) perform electronic records management;                    | 0 |   |  |
| (6) practice emergency destruction; and                       | 0 |   |  |
| (7) identify storage media protection and control procedures. | 0 |   |  |

**\*\* defined in C.F.R. 32 Section 2003, National Security Information - Standard Forms, March 30, 1987;**