APPENDIX A: INSTRUCTIONAL STRATEGIES (TRAINING DELIVERY METHODS)

Instructor-Led
The traditional instructional strategy is instructor-led and considered a group instruction strategy. This involves bringing students together into a common place, usually a classroom environment, with an instructor or facilitator. It can provide considerable interaction between the instructor and the students. It is usually the least expensive as far as designing and development of instructional material. However, it can be the most expensive during implementation, especially if it requires students to travel to a central location.

Text-Based
Text-based training is an individual, self-paced form of training. The student reads a standard textbook (or any book) on the training content. Text-based training does not allow for interaction with an instructor. However, the book’s information is usually written by an individual with expertise in the subject matter. In addition, students can access the material when it is needed and can review (or re-read) sections as needed.

Paper-Based or Workbook
Paper-based or workbook training is a type of individual, self-paced in-

PAYOFF IDEA
These appendices to “Making Security Awareness Happen” provide additional information to help the reader launch an effective security training program. Appendix A provides a detailed definition of instructor-led and technology-based training delivery methods. Appendix B contains more detailed information for each course, including the title, brief description, intended audience, high-level list of topics, and other information as appropriate.
struction. It is the oldest form of distance learning (i.e., correspondence courses). Workbooks include or instructional text, graphical illustrations, and practice exercises. The workbooks are written specifically to help students learn particular subjects or techniques. The practice exercises help students to remember what is covered in the books by giving them an opportunity to work with the content. In some cases, students may be required to complete a test or exam to show competency in the subject.

Video-Based
Video-based training is usually an individual, self-paced form of instruction. The information is provided on a standard VHS video cassette tape that can be played using a standard VHS video cassette recorder (VCR). If used as a self-paced form of instruction, it does not allow for interaction with the instructor. However, if used in the classroom, a video can be discussed and analyzed as an interactive exercise. Video does allow for animated graphics that can show processes or a demonstration of step-items. It is flexible as far as delivery time and location, and if necessary, can be repeated.

Technology-Based, Including CBT and WBT
Technology-based training is also an individual, self-paced instructional strategy. It is any training that uses a computer as the focal point for instructional delivery. With technology-based training, instructional content is provided through the use of a computer and software that guides a student through an instructional program.

This can be either computer-based training delivered via a floppy disk, CD-ROM, or loaded on a server; or Web-based training delivered via the Internet or an intranet.

Computer-based training (CBT) involves several presentation methods, including tutorials, practice exercises, simulations or emulations, demonstrations, problem-solving exercises, and games. CBT has many positive features that can be of importance to agencies that need to deliver a standard set of instructional material to a large group of students who are in geographically separate areas. The benefits of CBT include immediate feedback, student control of instructional material, and the integration of multimedia elements such as video, audio, sounds, and graphical animations.

After the initial CBT development costs, CBT can be used to teach any number of students at any time. Customized CBT programs can focus only on what students need to learn, thus training time and costs can be significantly reduced. In addition, CBT can enable one to reduce or eliminate travel for students; thus, total training costs can also be reduced. As a self-paced, individualized form of instruction, CBT provides flexibility
for the student. For example, the student can control the training environment by selecting specific lessons or topics. In addition, for some students, the anonymous nature can be nonthreatening.

Although CBT has many benefits, it is important to remember that CBT is not the answer to all training needs. It some situations, it can be more appropriate, effective, and cost-efficient. However, in other situations, it may produce a negative student attitude and destroy the goodwill and goals of the training program. For example, students who are offered CBT courses and instructed to fit it in to their schedule may believe they are expected to complete the training outside of the workday. These same students know that taking an instructor-led course allows them to complete the training during a workday. Therefore, they may view CBT as an unfair time requirement.

CBT includes computer-assisted learning (CAL), which uses a computer as a tool to aid in a traditional learning situation, such as classroom training. The computer is a device to assist the instructor during the training process, similar to an overhead projector or handouts. It also includes computer-assisted testing (CAT), which assesses an individual through the medium of a computer. Students take the test at the computer, and the computer records and scores the test. CAT is embedded in most computer-based training products.

Web-based training (WBT) is a new, creative method for delivering computer-based training to widespread, limitless audiences. WBT represents a shift from the current delivery of CBT. In the CBT format, the information is usually stored on the local machine, server, or a CD-ROM. In WBT, the information is distributed via the World Wide Web (WWW) and most likely is stored at a distant location or an agency’s central server. The information is displayed to the user using a software application called a browser, such as Internet Explorer. The content is presented by text, graphics, audio, video, and graphical animations. WBT has many of the same benefits as CBT, including saving time and easy access. However, one of the key advantages of WBT over CBT is the ease of updating information. If changes need to be made to instructional material, the changes are made once to the server, and then everyone can access the new information. The challenges of WBT are providing the technical capability for the student’s computer, the agency’s server, and the available bandwidth.

APPENDIX B: SUGGESTED IT SYSTEM SECURITY TRAINING COURSES (EXHIBIT 1)
INFOSEC 101 IT Security Basics

**Brief Description.** This course should describe the core terms and concepts that every user of the IT system must know, the fundamentals of IT security and how to apply them, plus the IT system security rules of behavior. This will allow all individuals to understand what their role is in protecting the IT systems assets and information.
# EXHIBIT 1 — Suggested Information System Security Training Courses

<table>
<thead>
<tr>
<th>Course Number and Content Level</th>
<th>Course Title</th>
<th>Intended Audience</th>
<th>Possible Prerequisite</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFOSEC 101 Basic</td>
<td>IT Security Basics</td>
<td>All employees</td>
<td>None</td>
</tr>
<tr>
<td>INFOSEC 102 Basic</td>
<td>IT Security Basics for Networks Processing Classified Information</td>
<td>All employees with access to a network processing classified information</td>
<td>None</td>
</tr>
<tr>
<td>INFOSEC 103 Basic</td>
<td>IT Security Basics — Annual Refresher</td>
<td>All employees</td>
<td>INFOSEC 101</td>
</tr>
<tr>
<td>INFOSEC 104 Basic</td>
<td>Fundamentals of IT Security</td>
<td>Individuals directly responsible for IT security</td>
<td>None</td>
</tr>
<tr>
<td>INFOSEC 201 Intermediate</td>
<td>Developing the IT System Security Plan</td>
<td>Individuals responsible for developing the IT system security plan</td>
<td>INFOSEC 101 or 103</td>
</tr>
<tr>
<td>INFOSEC 202 Intermediate</td>
<td>How to Develop an IT System Contingency Plan</td>
<td>Individuals responsible for developing the IT system contingency plan</td>
<td>INFOSEC 101 or 103</td>
</tr>
<tr>
<td>INFOSEC 203 Intermediate</td>
<td>System/Technical Responsibilities for Protecting the IT System</td>
<td>Individuals responsible for the planning and daily operations of the IT system</td>
<td>INFOSEC 101 or 103</td>
</tr>
<tr>
<td>INFOSEC 204 Intermediate</td>
<td>Life Cycle Planning for IT System Security</td>
<td>Managers responsible for the acquisition and design of the IT system</td>
<td>INFOSEC 101 or 103</td>
</tr>
<tr>
<td>INFOSEC 205 Intermediate</td>
<td>Basic Information System Security Officer (ISSO) Training</td>
<td>Individuals assigned as the ISSO or alternate ISSO</td>
<td>INFOSEC 101 or 103</td>
</tr>
<tr>
<td>INFOSEC 206 Intermediate</td>
<td>Certifying the IT System</td>
<td>Individuals responsible for the Designated Approving Authority (DAA) role</td>
<td>INFOSEC 101 or 103 INFOSEC 203</td>
</tr>
<tr>
<td>Course</td>
<td>Description</td>
<td>Audience</td>
<td>Prerequisites</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>INFOSEC 207 Intermediate</td>
<td>Information System Security for Executive Managers</td>
<td>Executive-level managers</td>
<td>None</td>
</tr>
<tr>
<td>INFOSEC 208 Intermediate</td>
<td>An Introduction to Network and Internet Security</td>
<td>Individuals responsible for network connections</td>
<td>INFOSEC 101 or 103 INFOSEC 203</td>
</tr>
<tr>
<td>INFOSEC 209</td>
<td>An Introduction to Cryptography</td>
<td>Individuals responsible for network connections information and security</td>
<td>INFOSEC 101 or 103 INFOSEC 203 or 205</td>
</tr>
<tr>
<td>INFOSEC 301 Advanced</td>
<td>Understanding Audit Logs</td>
<td>Individuals responsible for reviewing audit logs</td>
<td>INFOSEC 101 or 103 INFOSEC 203 or 205</td>
</tr>
<tr>
<td>INFOSEC 302 Advanced</td>
<td>Windows NT 4.0 Security</td>
<td>Individuals responsible for networks using Windows NT 4.0</td>
<td>INFOSEC 101 or 103 INFOSEC 203 or 205</td>
</tr>
<tr>
<td>INFOSEC 303 Advanced</td>
<td>Windows 2000 Security</td>
<td>Individuals responsible for networks using Windows 2000</td>
<td>INFOSEC 101 or 103 INFOSEC 203</td>
</tr>
<tr>
<td>INFOSEC 304 Advanced</td>
<td>UNIX Security</td>
<td>Individuals responsible for networks using UNIX</td>
<td>INFOSEC 101 or 103 INFOSEC 203</td>
</tr>
<tr>
<td>INFOSEC 305 Advanced</td>
<td>Advanced ISSO Training</td>
<td>Individuals assigned as the ISSO or alternate ISSO</td>
<td>INFOSEC 205</td>
</tr>
<tr>
<td>INFOSEC 306 Advanced</td>
<td>Incident Handling</td>
<td>Individuals responsible for handling IT security incidents</td>
<td>INFOSEC 101 or 103 INFOSEC 205</td>
</tr>
<tr>
<td>INFOSEC 307 Advanced</td>
<td>How to Conduct a Risk Analysis/Assessment</td>
<td>Individuals responsible for conducting risk analyses</td>
<td>INFOSEC 101 or 103 INFOSEC 205</td>
</tr>
</tbody>
</table>
**Intended Audience.** This course is intended for all employees who use the IT system, regardless of their specific job responsibilities. Essentially, all employees should receive this training.

**List of Topics.** What Is IT Security and Why Is It Important; Federal Laws and Regulations; Vulnerabilities, Threats, and Sensitivity of the IT System; Protecting the Information, Including Sensitive but Unclassified and Classified Information; Protecting the Hardware; Password Protections; Media Handling (i.e., how to process, store, and dispose of information on floppy disks); Copyright Issues; Laptop Security; User Accountability; Who to Contact with Problems; and other specific agency policies related to all users of the IT system. Note that if the agency processes classified information, a separate briefing should be given.

Note: Because most agencies will require this course for all employees, it is a good example of content that should be delivered via a technology-based delivery. This includes either video, computer-based training via CD-ROM, or Web-based training via the agency’s intranet.

INFOSEC 102 IT Security Basics for a Network Processing Classified Information

**Brief Description.** This course describes the core terms and concepts that every user of the IT system must know, the fundamentals of IT security and how to apply them, and the rules of behavior. It is similar to INFOSEC 101 except that it also provides information pertinent to employees who have access to a network processing classified information.

**Intended Audience.** This course is intended for all employees with access to a network processing classified information.

**List of Topics.** What Is IT Security and Why Is It Important; Federal Laws and Regulations; Vulnerabilities, Threats, and Sensitivity of the IT System; Protecting Classified Information; Protecting the Hardware, Including TEMPEST Equipment; Password Protections; Media Handling (i.e., how to process, store, and dispose of classified information); Copyright Issues; Laptop Security; User Accountability; Who to Contact with Problems; and other specific agency policies related to users of a classified IT system.

INFOSEC 103 IT Security Basics — Annual Refresher

**Brief Description.** This is a follow-on course to the IT Security Basics (INFOSEC 101). As technology changes, the demands and challenges for IT security also change. In this course, the agency will look at the most critical challenges for the end user. The focus of the refresher course will be on how to meet those needs.
Intended Audience. This course is for all employees who use the IT system.

List of Topics. The topics would be specific to the agency and the pertinent IT security challenges it faces.

INFOSEC 104 Fundamentals of IT Security

Brief Description. This course is designed for employees directly involved with protecting the IT system. It provides a basic understanding of the federal laws and agency-specific policies and procedures, the vulnerabilities and threats to IT systems, the countermeasures that can help to mitigate the threats, and an introduction to the physical, personnel, administrative, and system/technical controls.

Intended Audience. The course is for employees who need more than just the basics of IT security. It is an introductory course that can be used as a prerequisite for higher-level material. This could include System Administrators, System Staff, Information Officers, Information System Security Officers, Security Officers, and Program Managers.

Note: This course can be taken in place of the INFOSEC 101 course. It is designed as an introductory course for those employees who have job responsibilities directly related to securing the IT system.

INFOSEC 201 Developing the IT System Security Plan

Brief Description. By law, every IT federal system must have an IT system security plan for its general support systems and major applications. This course explains how to develop an IT System Security Plan following the guidelines set forth in NIST SP 800-18 “Guide for Developing Security Plans for Information Technology Systems.”

Intended Audience. The system owner (or team) responsible for ensuring that the IT system security plan is prepared and implemented. In many agencies, the IT system security plan will be developed by a team, such as the System Administrator, Information Officer, Security Officer, and the Information System Security Officer.

List of Topics. System Identification; Assignment of Security Responsibilities; System Description/Purpose; System Interconnection; Sensitivity and Sharing of Information; Risk Assessment and Management; Administrative, Physical, Personnel, and System/Technical Controls; Life Cycle Planning; and Security Awareness and Training.

Note: The design of this course should be customized with an agency-approved methodology and a predefined set of templates on how to de-
velop an IT system security plan. The students should leave the class with agency-approved tools necessary to develop the plan.

INFOSEC 202 How to Develop an IT System Contingency Plan

Brief Description. The hazards facing IT systems demand that effective business continuity plans and disaster-recovery plans be in place. Business continuity plans define how to recover from disruptions and continue support for critical functions. Disaster recovery plans define how to recover from a disaster and restore critical functions to normal operations. The first step is to define one's agency's critical functions and processes, and determine the recovery timeframes and trade-offs. This course discusses how to conduct an in-depth Business Impact Analysis (BIA) (identifying the critical business functions within an agency and determining the impact of not performing the functions beyond the maximum acceptable outage) that defines recovery priorities, processing interdependencies, and the basic technology infrastructure required for recovery.

Intended Audience. Those employees responsible for the planning and management of the IT system. This may include the System Administrator, Information Officer, Security Officer, and Information System Security Officer.

List of Topics. What Is an IT System Contingency Plan; Conducting a Business Impact Analysis (BIA); Setting Your Site (hot site, cold site, warm site); Recovery Objectives; Recovery Requirements; Recovery Implementation; Backup Options and Plans; Testing the Plan; and Evaluating the Results of Recovery Tests.

Note: The content of this course should be customized with an agency-approved methodology for creating an IT system contingency plan. If possible, preapproved templates or tools should be included.

INFOSEC 203 System/Technical Responsibilities for Protecting the IT System

Brief Description. This course begins by explaining the vulnerabilities of and threats to the IT system and what is necessary to protect the physical assets and information. It focuses on specific requirements such as protecting the physical environment, installing software, access controls, configuring operating systems and applications to meet security requirements, and understanding audit logs.

Intended Audience. Employees who are involved and responsible for the planning and day-to-day operations of the IT system. This would include System Administrators, System Staff, Information Officers, and Information System Security Officers.
List of Topics. Overview of IT System Security; Identifying Vulnerabilities, Threats, and Sensitivity of the IT System; Identifying Effective Countermeasures; Administrative Responsibilities (e.g., management of logs and records); Physical Responsibilities (e.g., server room security); Interconnection Security; Access Controls (identification and authentication); Group and File Management (setting up working groups and shared files); Group and File Permissions (configuring the system for access permissions); Audit Events and Logs; and IT Security Maintenance.

INFOSEC 204 Life Cycle Planning for IT System Security

Brief Description. The system life cycle is a model for building and operating an IT system from its inception to its termination. This course covers the fundamentals of how to identify the vulnerabilities of and threats to IT systems before they are implemented and how to plan for IT security during the acquisition and design of an IT system. This includes identifying the risks that may occur during implementation of the IT system and how to minimize those risks, describing the standard operating procedures with a focus on security, how to test that an IT system is secure, and how to dispose of terminated assets.

Intended Audience. This course is designed for managers tasked with the acquisition and design of IT systems. This could include Contracting Officers, Information Officers, System Administrators, Program Managers, and Information System Security Officers.

List of Topics. Identify IT Security Needs During the Design Process; Develop IT Security in the Acquisition Process; Federal Laws and Regulations; Agency Policies and Procedures; Acquisition, Development, Installation, and Implementation Controls; Risk Management; Establishing Standard Operating Procedures; and Destruction and Disposal of Equipment and Media.

Note: The course focus should be on the implementation and use of organizational structures and processes for IT security and related decision-making activities. Agency-specific policies, guidelines, requirements, roles, responsibilities, and resource allocations should be previously established.

INFOSEC 205 Basic Information System Security Officer (ISSO) Training

Brief Description. This course provides an introduction to the ISSO role and responsibilities. The ISSO implements the IT system security plan and provides security oversight on the IT system. The focus of the course is on understanding the importance of IT security and how to provide a security management role in the daily operations.
**Intended Audience.** Employees assigned as the ISSO or equivalent. This could be System Administrators, Information Officers, Program Managers, or Security Officers.

**List of Topics.** Overview of IT Security; Vulnerabilities, Threats, and Sensitivity; Effective Countermeasures; Administrative Controls; Physical Controls; Personnel Controls; System/Technical Controls; Incident Handling; and Security Awareness Training.

Note: Each agency should have someone designated as the Information System Security Officer (ISSO) who is responsible for providing security oversight on the IT system.

INFOSEC 206 Certifying and Accrediting the IT System

**Brief Description.** This course provides information on how to verify that an IT system complies with information security requirements. This includes granting final approval to operate an IT system in a specified security mode and ensure that classified or sensitive but unclassified (SBU) information is protected according to federal and agency requirements.

**Intended Audience.** Individuals assigned the Designated Approving Authority (DAA) role and responsibilities. This includes Program Managers, Security Officers, Information Officers, or Information System Security Officers.

**List of Topics.** Federal Laws and Regulations; Agency Policies and Procedures; Understanding Vulnerabilities, Threats, and Sensitivities; Effective Countermeasures; Access Controls; Groups and File Permissions; Protection of Classified and SBU Information; Protection of TEMPEST and Other Equipment; The Accreditation Process; Incident Handling; Life Cycle Management; Standard Operating Procedures; and Risk Management.

INFOSEC 207 Information System Security for Executive Managers

**Brief Description.** This course provides an overview of the information system security concerns for executive-level managers. It emphasizes the need for both planning and managing security on the IT system, how to allocate employee and financial resources, and how to lead the IT security team by example.

**Intended Audience.** Executive-level managers.

**List of Topics.** Overview of IT System Security; Federal Laws and Regulations; Vulnerabilities and Threats to the IT System; Effective Countermeasures; Need for IT Security Management and Oversight; and Budgeting for IT Security.
Note: This course content should be customized for each agency to make sure it meets the specific needs of the executive-level management team. It is anticipated that this would be several short, interactive sessions based on specific topics. Some sessions could be delivered via a technology-based application to effectively plan for time limitations.

INFOSEC 208 An Introduction to Network and Internet Security

**Brief Description.** In this course, the focus is on how develop a network and Internet/intranet security policy to protect the agency’s IT system assets and information. The focus is on how to analyze the vulnerabilities of the IT system and review the various external threats, how to manage the risks and protect the IT system from unauthorized access, and how to reduce one’s risks by deploying technical countermeasures such as firewalls and data encryption devices.

**Intended Audience.** Employees involved with the implementation, day-to-day management, and oversight responsibilities of the network connections, including internal intranet and external Internet connections. This could include System Administrators, System Staff, Information Officers, Information System Security Officers, Security Officers, and Program Managers.

**List of Topics.** Overview of IT Network Security and the Internet; Introduction to TCP/IP and Packets; Understanding Vulnerabilities and Threats to Network Connections (hackers, malicious codes, spoofing, sniffing, denial-of-service attacks, etc.); Effective Countermeasures for Network Connections (policies, access controls, physical protections, anti-virus software, firewalls, data encryption, etc.); Developing a Network and Internet/intranet Security Policy; and How to Recognize an Internet Attack.

INFOSEC 209 An Introduction to Cryptography

**Brief Description.** The focus of this course is to provide an overview of cryptography. This includes the basic concepts of cryptography, public and private key algorithms in terms of their applications and uses, key distribution and management, the use of digital signatures to provide authenticity of electronic transactions, and non-repudiation.

**Intended Audience.** Employees involved with the management and security responsibilities of the network connections. This could include System Administrators, System Staff, Information Officers, Information System Security Officers, Security Officers, and Program Managers.

**List of Topics.** Cryptography Concepts; Authentication Methods Using Cryptographic Modules; Encryption; Overview of Certification Authority;
DATA SECURITY MANAGEMENT

Digital Signatures; Non-repudiation; Hash Functions and Message Digests; Private Key and Public Key Cryptography; and Key Management.

INFOSEC 301 Understanding Audit Logs

**Brief Description.** This is an interactive class focusing on how to understand and review audit logs. It explains what types of events are captured in an audit log, how to search for unusual events, how to use audit log tools, how to record and store audit logs, and how to handle an unusual audit event.

**Intended Audience.** Employees assigned to manage and provide oversight of the daily IT system operations. This includes System Administrators, Information Officers, and Information System Security Officers.

**List of Topics.** Understanding an IT System Event, Planning for Audit Log Reviews; How to Review Audit Logs; How to Find and Search Through Audit Logs; Using Third-Party Tools for Audit Log Reviewing; How to Handle an Unusual System Event in the Audit Log.

Note: As a prerequisite, students should have completed either INFOSEC 203 or INFOSEC 205 so that they have a basic understanding of IT security concepts.

INFOSEC 302 Windows NT 4.0 Server and Workstation Security

**Brief Description.** This course focuses on how to properly configure the Windows NT 4.0 security features for both the server and workstation operating systems. Students learn the security features of Windows NT and participate in installing and configuring the operating systems in a hands-on computer lab.

**Intended Audience.** This course is designed for employees who are responsible for installing, configuring, and managing networks using the Windows NT 4.0 server and workstation operating system. This may include Information Officers, System Administrators, and System Staff.

**List of Topics.** Overview of the Windows NT 4.0 Server and Workstation Operating Systems; Identification and Authentication Controls; Discretionary Access Controls; Group Organization and Permissions; Directory and File Organization and Permissions; Protecting System Files; Auditing Events; Using the Windows NT Tools to Configure and Maintain the System.

Note: As a prerequisite, students should complete INFOSEC 203 so they have a basic understanding of IT security concepts.

INFOSEC 303 Windows 2000 Security

**Brief Description.** This course is similar to INFOSEC 302 except that it focuses on how to properly configure the security features of the Win-
Windows 2000 operating system. Students learn the security features of Windows 2000 by installing and configuring the operating system in a hands-on computer lab.

**Intended Audience.** This course is designed for employees who are responsible for installing, configuring, and managing networks using the Windows 2000 operating system. This may include Information Officers, System Administrators, and System Staff.

**List of Topics.** Overview of the Windows 2000 Operating System; The Domain Name System (DNS); Migrating Windows NT 4.0 Domains; Identification and Authentication Controls; Discretionary Access Controls; File System Resources (NTFS); Group Organization and Permissions; Directory and File Organization and Permissions; Protecting System Files; Auditing Events; Using the Windows 2000 Tools to Configure and Maintain the System.

Note: As a prerequisite, students should complete INFOSEC 203 so they have a basic understanding of IT security concepts.

**INFOSEC 304 Unix Security**

**Brief Description.** In this hands-on course, students will gain the knowledge and skills needed to implement security on the UNIX operating system. This includes securing the system from internal and external threats, protecting the UNIX file system, controlling superuser access, and configuring tools and utilities to minimize vulnerabilities and detect intruders.

**Intended Audience.** This course is designed for employees who are responsible for installing, configuring, and managing networks using the UNIX operating system. This may include Information Officers, System Administrators, and System Staff.

**List of Topics.** Introduction to UNIX Security; Establishing Secure Accounts; Storing Account Information; Controlling Root Access; Directory and File Permissions; Minimize Risks from Unauthorized Programs; and Understanding TCP/IP and Security.

Note: As a prerequisite, students should complete INFOSEC 203 so that they have a basic understanding of IT security concepts.

**INFOSEC 305 Advanced ISSO Training**

**Brief Description.** This course provides an in-depth look at the ISSO responsibilities. The focus is on how to review security plans, contingency plans/disaster recover plans, and IT system accreditation; how to handle IT system incidents; and how specific IT security case studies are examined and evaluated.
**Intended Audience.** This is intended for ISSOs who have completed INFOSEC 205 and have at least one year of experience as the ISSO.

**List of Topics.** Oversight Responsibilities for Reviewing IT System Security Plans and Contingency Plans; How to Handle IT System Incidents; and Case Studies.

INFOSEC 306 Incident Handling

**Brief Description.** This course explains the procedures for handling an IT system security incident. It begins by defining how to categorize incidents according to risk, followed by how to initiate and conduct an investigation and who to contact for support. Key to handling incidents is ensuring that equipment and information is not compromised during an investigation. Thus, students learn the proper procedures for safekeeping assets and information.

**Intended Audience.** This course is designed for employees who are responsible for handling IT security incidents. This could include Information Officers, Information System Security Officers, Security Officers, and individuals representing a computer incident response team.

**List of Topics.** Understanding an IT System Security Incident; Federal Laws and Civil/Criminal Penalties; Agency Policies and Penalties; The Agency-Specific Security Incident Reporting Process; Security Investigation Procedures; Identify Investigative Authorities; Interfacing with Law Enforcement Agencies; Witness Interviewing; Protecting the Evidence; and How to Write an IT System Security Incident Report.

Note: As a prerequisite, students should complete INFOSEC 205 so that they have a basic understanding of IT security concepts.

INFOSEC 307 How to Conduct a Risk Analysis/Assessment

**Brief Description.** This course explains the process of conducting a risk analysis/assessment. It reviews why a risk analysis is important, the objectives of a risk analysis, when the best time is to conduct a risk analysis, the different methodologies to conduct a risk assessment (including a review of electronic tools) and provides plenty of hands-on opportunities to complete a sample risk analysis. A critical element of a risk analysis/assessment is considering the target analysis and target assessment. The unauthorized intruder may also be conducting an analysis of the information system risks and will know the vulnerabilities to attack.

**Intended Audience.** Individuals tasked with completing a risk analysis. This could include the Information Officer, System Administrator, Program Manager, Information System Security Officer, and Security Officer.
List of Topics. Overview of a Risk Analysis; Understanding Vulnerabilities, Threats, and Sensitivity and Effective Countermeasures of IT Systems; Objectives of a Risk Analysis; Risk Analysis Methodologies; Federal Guidance on Conducting a Risk Analysis; Process of Conducting a Risk Analysis; Electronic Risk Analysis Tools; Completing Sample Risk Analysis Worksheets (asset valuations, threat, and vulnerability evaluation; level of risk; and countermeasures); and Reviewing Target Analysis/Assessments.

Note: This course may be offered in conjunction with INFOSEC 201 and INFOSEC 206.

Susan D. Hansche, CISSP, is a senior manager for Information System Security Awareness and Training at TROY Systems, Inc., based in Fairfax, Virginia. She has designed numerous training courses on information technology and information system security for both private-sector and government clients. She can be reached via e-mail at shansche@troy.com.