

## **DOE CYBER SECURITY:**

### **CORE COMPETENCY TRAINING REQUIREMENTS**

#### **Key Cyber Security Role: Information System Security Officer (ISSO)**

*Role Definition:* The ISSO is the individual responsible to the ISSM, information owner, and System Owner for ensuring the appropriate operational security posture is maintained for an information system.

*Competency Area:* **Data Security**

*Functional Requirement:* **Implement**

*Competency Definition:* Refers to the application of the principles, policies, and procedures necessary to ensure the confidentiality, integrity, availability, and privacy of data in all forms of media (i.e., electronic and hardcopy) throughout the data life cycle.

*Behavioral Outcome:* The individual serving as an ISSO will understand the policies and procedures required to protect all categories of information as well as have a working knowledge of data access controls implemented to ensure the confidentiality, integrity, and availability of information.

*Training concepts to be addressed at a minimum (additional detailed training accomplished as required based on site-specific functional responsibilities):*

- Apply and verify data security access controls, privileges, and associated profiles.
- Implement media control procedures and continuously monitor for compliance.
- Implement and verify data security access controls and assign privileges based on need-to-know.
- Investigate all suspected cyber security incidents in accordance with Departmental directives and applicable PCSPs.
- Apply and maintain required confidentiality controls and processes.
- Implement authenticator generation and verification requirements and processes.
- Execute media sanitization (i.e., clearing, purging, or destroying) and reuse procedures.
- Execute processes and procedures for protecting SUI, including PII.

*Training Evaluation Criteria:* **Demonstrate**

*Methods of Demonstration:* **Examination; Simulation; Desk Top Analysis; On-the-Job-Training**

*Level of Demonstration:*

**General** – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

**Functional** – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

**Detailed** – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **functional** knowledge of DOE/PCSP data security policies, processes, and procedures.
- Demonstrate a **functional** knowledge of DOE/PCSP incident management, sanitization, authenticator, and SUI protection policies and technical requirements
- Demonstrate a **detailed** knowledge of Operating Unit data security policies, processes, and procedures
- Demonstrate a **detailed** ability to apply Operating Unit policy and technical requirements for incident reporting, media sanitization and reuse, authenticator generation and distribution, and SUI protection
- Demonstrate a **detailed** knowledge of the security capabilities of the systems for which they are responsible
- Demonstrate a **detailed** ability to apply security measures to the systems for which they are responsible

*Competency Area:* **Incident Management**

*Functional Requirement:* **Implement**

*Competency Definition:* Refers to the knowledge and understanding of the processes and procedures required to prevent, detect, investigate, contain, eradicate, and recover from incidents that impact the organizational mission as directed by the DOE Cyber Incident Response Capability (CIRC).

*Behavioral Outcome:* The individual serving as an ISSO will understand the policies, procedures, and processes for identifying, categorizing, investigating, isolating, assessing, and reporting cyber security incidents in coordination with other impacted organizations as dictated by DOE CIRC.

*Training concepts to be addressed at a minimum (additional detailed training accomplished as required based on site-specific functional responsibilities):*

- Apply response actions in reaction to security incidents in accordance with established policies, plans, and procedures to include appropriate incident characterization (i.e., Type 1 or Type 2) and categorization (i.e., low, medium, high, or very high).
- Respond to and report potential incidents to the ISSM within mandated timeframes as required by the DOE CIRC and other federal agencies (e.g., Office of Health, Safety, and Security).
- Perform assessments to determine the impact of the loss of confidentiality, integrity, and/or availability.
- Respond proactively to information and alerts disseminated by the DOE CIRC to include performing consequence analyses and corrective actions.
- Assist in collecting, processing, and preserving evidence according to Departmental/PCSP standards, procedures, directives, policies, and regulations and laws (statutes).
- Follow proper chain-of-custody best practices in accordance with procedures set forth by the DOE CIRC.
- Collect and retain audit data to support technical analysis relating to misuse, penetration, reconstruction, or other investigations.
- Provide audit data to appropriate law enforcement or other investigating agencies, to include Departmental security elements.
- Execute incident response plans.

- Execute penetration testing activities and incidence response exercises.
- Ensure lessons learned from incidents are collected in a timely manner and are incorporated into plan reviews.
- Collect, analyze, and report incident management measures.

*Training Evaluation Criteria: **Demonstrate***

*Methods of Demonstration: **Examination; Simulation; Desk Top Analysis***

*Level of Demonstration:*

**General** – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

**Functional** – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

**Detailed** – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **functional** knowledge of DOE/PCSP incident management security policies, processes, and procedures
- Demonstrate a **detailed** knowledge of Operating Unit incident management policies, plans, and procedures
- Demonstrate a **detailed** ability to appropriately characterize and categorize incidents
- Demonstrate a **detailed** knowledge of reporting and documentation requirements for Incident Management and Reporting
  - DOE-CIRC
  - Inspector General
  - Office of Intelligence and Counter-intelligence
  - Federal Bureau of Investigation
  - Local Law Enforcement
- Demonstrate a **detailed** knowledge of methods for evidence preservation and chain of custody
- Demonstrate a **detailed** ability to use penetration testing tools to identify vulnerabilities
- Demonstrate a **detailed** ability to analyze and evaluate collected information concerning events to provide incident recognition and reporting

*Competency Area: **Cyber Security Training and Awareness***

*Functional Requirement: **Implement***

*Competency Definition:* Refers to the knowledge of principles, practices, and methods required to raise employee awareness about basic information security and train individuals with information security roles to increase their knowledge, skills, and abilities.

*Behavioral Outcome:* The individual serving as an ISSO will have the knowledge required to deliver cyber awareness and training material to general users based on an identified need and/or organizational policies and within organizational time frames.

*Training concepts to be addressed at a minimum (additional detailed training accomplished as required)*

*based on site-specific functional responsibilities):*

- Identify existing awareness and training materials that are appropriate and timely for general users to include formal acceptance of his/her responsibility (e.g., Code of Conduct).
- Deliver awareness and training to general users based on identified needs and within DOE mandated time frames.
- Communicate management's commitment and the importance of cyber security awareness and training to general users.

*Training Evaluation Criteria: **Demonstrate***

*Methods of Demonstration: **Examination; Simulation; Desk Top Analysis***

*Level of Demonstration:*

**General** – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

**Functional** – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

**Detailed** – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **general** knowledge of all DOE/PCSP cyber security policies, processes, and procedures
- Demonstrate a **functional** ability to identify user training needs
- Demonstrate a **functional** ability to provide training to the user community on the systems for which they are responsible

*Competency Area: **Information Technology (IT) Systems Operations and Maintenance***

*Functional Requirement: **Implement***

*Competency Definition:* Refers to the ongoing application of principles, policies, and procedures to maintain, monitor, control, and protect IT infrastructure and the information residing on such infrastructure during the operations phase of an IT system or application. Individuals with these functions perform a variety of data collection, analysis, reporting and briefing activities associated with security operations and maintenance to ensure that the organizational security policies are implemented and maintained on information systems.

*Behavioral Outcome:* The individual serving as an ISSO will understand the policies, procedures, and controls required to protect IT infrastructure and data and will be able to apply and assess technical, operational, and/or administrative security controls as mandated by Departmental/PCSP standards.

*Training concepts to be addressed at a minimum (additional detailed training accomplished as required based on site-specific functional responsibilities):*

- Perform security administration processes and procedures in accordance with Departmental/PCSP standards, procedures, directives, policies, and regulations and laws (statutes).

- Establish a secure computing environment by monitoring, controlling, and managing unauthorized changes in system configuration, software, and hardware.
- Perform monitoring and analysis of system audit records for indications of inappropriate or unusual activity.
- Perform security performance testing and reporting and recommend security solutions in accordance with Departmental/PCSP standards, procedures, directives, policies, and regulations and laws (statutes).
- Perform security administration changes and validation testing.
- Uniquely identify (i.e., label), control, and track all IT configuration items through the continuous monitoring process.
- Uniquely identify configuration changes and maintain a history of the change control methodology and tools used for information systems with security categories of Moderate and High and for all National Security Systems (NSS)
- Collaborate with technical support, incident management, and security engineering teams to develop, implement, control, and manage new security administration technologies.
- Monitor vendor agreements and Service Level Agreements (SLA) to ensure that contract and performance measures are achieved.
- Perform security testing.
- Create a Plan of Actions and Milestones (POA&M) for correction of vulnerabilities as required by Departmental standards or applicable PCSPs.

*Training Evaluation Criteria:* **Demonstrate**

*Methods of Demonstration:* **Examination; Simulation; Desk Top Analysis; On-the-Job**

*Level of Demonstration:*

**General** – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

**Functional** – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

**Detailed** – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **functional** knowledge of DOE/PCSP cyber security policies, processes, and procedures involving configuration management, SDLC, continuous monitoring, and FISMA reporting
- Demonstrate a **detailed** knowledge of Operating Unit cyber security policy, plans, and procedures involving configuration management, SDLC, continuous monitoring, and FISMA reporting
- Demonstrate a **detailed** ability to apply Operating unit policy, plans, and procedures involving configuration management, SDLC, continuous monitoring, and FISMA reporting to secure the systems for which they are responsible
- Demonstrate a **detailed** knowledge of the security features and issues for the systems for which they are responsible
- Demonstrate a **detailed** ability to perform compliance and performance tests of controls implemented for systems for which they are responsible
- Demonstrate a **general** knowledge of project management as it applies to SLAs, POA&Ms, contracts, security administration, and control testing

- Demonstrate a **detailed** ability to analyze events or test results and prepare a POA&M
- Demonstrate the **ability** to integrate project management, configuration management, continuous monitoring, and POA&M processes.
- Demonstrate a **detailed** ability to prepare reports identifying the results of compliance and performance tests

*Competency Area:* **Network and Telecommunications Security and Remote Access**

*Functional Requirement:* **Implement**

*Competency Definition:* Refers to application of the principles, policies, and procedures involved in ensuring the security of basic network and telecommunications services and data and in maintaining the hardware layer on which the data resides. Examples of these practices include perimeter defense strategies, defense-in-depth strategies, and data encryption techniques.

*Behavioral Outcome:* The individual serving as an ISSO will understand the policies, procedures, and controls required to protect network and telecommunication services and will be able to apply and assess technical, operational, and administrative security controls as mandated by Departmental/PCSP standards.

*Training concepts to be addressed at a minimum (additional detailed training accomplished as required based on site-specific functional responsibilities):*

- Prevent and detect intrusions and protect against malware.
- Perform audit tracking and reporting.
- Test strategic network security technologies for effectiveness.
- Monitor and assess network security vulnerabilities and threats using various technical and non-technical data.
- Mitigate network security vulnerabilities as prioritized by the organization in response to problems identified in vulnerability reports.
- Document interconnected system specifics (e.g., purpose, risk, information types, technical implementation, etc.) in accordance with Departmental directives and applicable PCSPs.
- Implement policies, procedures, and minimum security controls for the use of External Information Systems, wireless information technology, and portable/mobile devices in accordance with Departmental directives and applicable PCSPs.
- Implement policies and procedures related to Peer-to-Peer (P2P) networking in accordance with Departmental directives and applicable PCSPs.

*Training Evaluation Criteria:* **Demonstrate**

*Methods of Demonstration:* **Examination; Simulation; Desk Top Analysis**

*Level of Demonstration:*

**General** – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

**Functional** – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

**Detailed** – Demonstrates an understanding of the inner workings of individual parts of the

process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **functional** knowledge of DOE/PCSP cyber security networking policies, processes, and procedures
- Demonstrate a **detailed** knowledge of Operating Unit networking policies, processes, and procedures
- Demonstrate a **functional** knowledge of wired and wireless networking technologies and their security issues
- Demonstrate a **functional** knowledge of threats associated with networking information systems and controls to counter those threats
- Demonstrate a **detailed** knowledge of Operating Unit policy for interconnecting to non-government systems and information sharing technologies
- Demonstrate a **detailed** knowledge of the security capability of the system/network for which they are responsible.
- Demonstrate a **detailed** ability to identify security issues from audit logs and track down any impacts to the confidentiality, availability, or integrity of the system or information
- Demonstrate a **detailed** ability to conduct testing and analysis of applied controls on the system for which they are responsible

*Competency Area:* **Personnel Security**

*Functional Requirement:* **Implement**

*Competency Definition:* Refers to the knowledge of human resource selection methods and controls used by an organization to help deter willful acts of security breaches such as theft, fraud, misuse, and noncompliance. These controls include organization/functional design elements such as separation of duties, job rotation, and classification.

*Behavioral Outcome:* The individual serving as an ISSO will be knowledgeable of Personnel Security policies and procedures and will coordinate with the appropriate security offices to ensure that general users have the required security clearances and need-to-know authorizations before accessing information systems.

*Training concepts to be addressed at a minimum (additional detailed training accomplished as required based on site-specific functional responsibilities):*

- Coordinate with the personnel security office to ensure that background investigations and clearances are successfully completed based on position sensitivity requirements before access is granted to an IT system.
- Coordinate with physical security, IT security operations, and other impacted organizations when an employee's access to physical facilities, media, and information systems has been modified or terminated upon reassignment, change of duties, resignation, or termination.

*Training Evaluation Criteria:* **Demonstrate**

*Methods of Demonstration:* **Examination; Desk Top Analysis**

*Level of Demonstration:*

**General** – Demonstrates an overall understanding of the purpose and objectives of the

process/topic adequate to discuss the subject or process with individuals of greater knowledge  
**Functional** – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

**Detailed** – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **functional** knowledge of DOE/PCSP and Operating Unit cyber security policies, processes, and procedures involving position sensitivity
- Demonstrate a **detailed** knowledge of the procedures used to grant access to systems for which they are responsible
- Demonstrate a **detailed** knowledge of the procedures used to terminate access to systems for which they are responsible

*Competency Area:* **Physical and Environmental Security**

*Functional Requirement:* **Implement**

*Competency Definition:* Refers to the knowledge of controls and methods used to protect an organization's operational environment including personnel, computing equipment, data, and physical facilities. This concept also refers the methods and controls used to proactively protect an organization from natural or man-made threats to physical facilities, as well as physical locations where IT equipment is located (e.g., central computing facility).

*Behavioral Outcome:* The individual serving as an ISSO will be knowledgeable of Physical Security policies and procedures and will coordinate with the appropriate security offices to ensure that physical controls are implemented as mandated by Departmental/PCSP standards.

*Training concepts to be addressed at a minimum (additional detailed training accomplished as required based on site-specific functional responsibilities):*

- Control access to information assets in accordance with Departmental/PCSP standards, procedures, directives, policies, and regulations and laws (statutes).
- Integrate physical security concepts into test plans, procedures, and exercises.
- Conduct threat and vulnerability assessments to identify physical and environmental risks and vulnerabilities and update applicable controls as necessary.

*Training Evaluation Criteria:* **Demonstrate**

*Methods of Demonstration:* **Examination; Desk Top Analysis**

*Level of Demonstration:*

**General** – Demonstrates an overall understanding of the purpose and objectives of the

process/topic adequate to discuss the subject or process with individuals of greater knowledge  
**Functional** – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

**Detailed** – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **functional** knowledge of DOE/PCSP and Operating Unit cyber security policies, processes, and procedures involving the physical environment for information systems
- Demonstrate a **functional** knowledge of the system categorization/characterization methodology to determine impact utilizing physical threats and vulnerabilities to assess risk to the information system
- Demonstrate a **detailed** knowledge of control implementation methods to mitigate vulnerabilities and risk
- Demonstrate a **functional** knowledge physical security testing procedures and the utilization of exercises

*Competency Area:* **Regulatory and Standards Compliance**

*Functional Requirement:* **Implement**

*Competency Definition:* Refers to the application of the principles, policies, and procedures that enable an organization to meet applicable information security laws, regulations, standards, and policies to satisfy statutory requirements, perform industry-wide best practices, and achieve information security program goals.

*Behavioral Outcome:* The individual serving as an ISSO will understand the policies and procedures in place to ensure organizational compliance with applicable laws, regulations, and/or Departmental/PCSP requirements and will be able to monitor and audit information security controls, processes, and procedures to assess compliance.

*Training concepts to be addressed at a minimum (additional detailed training accomplished as required based on site-specific functional responsibilities):*

- Monitor, assess, and report information security compliance practices for organizational information systems in accordance with policies and procedures.
- Maintain ongoing and effective communications with key stakeholders for compliance reporting purposes.
- Conduct internal audits to determine if information security control objectives, controls, processes, and procedures are effectively applied and maintained and perform as expected.
- Document information security audit and assessment results, recommend remedial actions and procedures, and estimated due dates for completion of remedial actions in the POA&M and in corrective action plans as required.

*Training Evaluation Criteria:* **Demonstrate**

*Methods of Demonstration:* **Examination; Simulation; Desk Top Analysis**

*Level of Demonstration:*

**General** – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

**Functional** – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g.,

technical, legal, safety) or consult appropriate reference materials

**Detailed** – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **functional** knowledge of DOE/PCSP cyber security policies, processes, and procedures
- Demonstrate a **detailed** knowledge of Operating Unit cyber security policies, processes, and procedures
- Demonstrate a **functional** knowledge of Operating Unit mission/task involving the systems for which they are responsible
- Demonstrate a **detailed** ability to perform audit review and analysis to determine control implementation, effective operation, and any remedial actions
- Demonstrate a **detailed** ability to prepare assessment reports and needed POA&Ms

*Competency Area:* **Security Risk Management**

*Functional Requirement:* **Design**

*Competency Definition:* Refers to the knowledge of policies, processes, and technologies used to create a balanced approach to identifying and assessing risks to information assets, personnel, facilities, and equipment, and to manage mitigation strategies that achieve the security needed at an affordable cost.

*Behavioral Outcome:* The individual serving as an ISSO will understand organizational risk management policies and procedures and will be able to develop and conduct Security Test and Evaluation (ST&E) activities for systems under his/her purview based on identified operational risk.

*Training concepts to be addressed at a minimum (additional detailed training accomplished as required based on site-specific functional responsibilities):*

- Develop a Security Test and Evaluation (ST&E) process for evaluating the functionality and effectiveness of each system's security controls.
- Develop a risk assessment process for identifying and assessing environmental (i.e., operational, logical, or physical) and system risks to information assets, personnel, facilities, and equipment and evaluating mitigation strategies.

*Training Evaluation Criteria:* **Demonstrate**

*Methods of Demonstration:* **Examination; Simulation; Desk Top Analysis**

*Level of Demonstration:*

**General** – Demonstrates an overall understanding of the purpose and objectives of the

process/topic adequate to discuss the subject or process with individuals of greater knowledge

**Functional** – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

**Detailed** – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **detailed** knowledge of testing and evaluation methodologies and when each is applicable
- Demonstrate a **functional** knowledge of the DOE/PCSP and Operating Unit policies and procedures for evaluating and managing risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation.
- Demonstrate a **detailed** knowledge to identify applicability of risk management techniques.

*Competency Area:* **Security Risk Management**

*Functional Requirement:* **Implement**

*Competency Definition:* Refers to the knowledge of policies, processes, and technologies used to create a balanced approach to identifying and assessing risks to information assets, personnel, facilities, and equipment, and to manage mitigation strategies that achieve the security needed at an affordable cost.

*Behavioral Outcome:* The individual serving as an ISSO will understand organizational risk management policies and procedures and will be able to apply system controls based on system category, accreditation boundary, and identified risk in an effort to achieve the desired organizational risk posture.

*Training concepts to be addressed at a minimum (additional detailed training accomplished as required based on site-specific functional responsibilities):*

- Apply controls for each information system by determining the system category (e.g., high, medium, low, or Protection Index) as directed by Departmental directives or applicable PCSPs.
- Establish accreditation boundaries based on the system category, information confidentiality, and the form of accreditation (i.e., system, type or site accreditation).
- Determine if proposed changes will introduce new vulnerabilities or negate the mitigation of existing risks (i.e., security significant changes).
- Provide input to policies, plans, procedures, and technologies to balance the level of risk associated with benefits provided by mitigating controls.
- Assess possible threats and vulnerabilities to identify security risks and regularly update applicable security controls.
- Identify risk/functionality tradeoffs and work with stakeholders to ensure that risk management implementation is consistent with desired organizational risk posture.

*Training Evaluation Criteria:* **Demonstrate**

*Methods of Demonstration:* **Examination; Simulation; Desk Top Analysis**

*Level of Demonstration:*

**General** – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

**Functional** – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

**Detailed** – Demonstrates an understanding of the inner workings of individual parts of the

process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **functional** knowledge of the DOE/PCSP and Operating Unit policies and procedures for evaluating and managing risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation.
- Demonstrate a **functional** ability to evaluate the applicability of threats and vulnerabilities to the information system
- Demonstrate a **detailed** ability to evaluate risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation
- Demonstrate a **detailed** knowledge of controls needed based on system categorization/ characterization and evaluation of risk
- Demonstrate a **detailed** ability to apply controls without causing additional/new vulnerabilities for the information system

*Competency Area:* **System and Application Security**

*Functional Requirement:* **Design**

*Competency Definition:* Refers to the knowledge of principles, practices, and procedures required to integrate information security into an Information Technology (IT) system or application during the System Development Life Cycle (SDLC). The goal of this activity is to ensure that the operation of IT systems and software does not present undue risk to the organization and information assets. Supporting activities include risk assessment, risk mitigation, security control selection, implementation and evaluation, certification and accreditation (C&A), and software security standards compliance.

*Behavioral Outcome:* The individual serving as an ISSO will understand SDLC policies and processes and will integrate applicable information security requirements and C&A documentation requirements into the application design process.

*Training concepts to be addressed at a minimum (additional detailed training accomplished as required based on site-specific functional responsibilities):*

- Identify accreditation boundaries and form of accreditation.
- Integrate applicable information security requirements, controls, processes, and procedures into information system and application design specifications in accordance with Departmental and/or PCSP established standards, policies, procedures, guidelines, directives, and regulations and laws (statutes).
- Specify the requirements and responsibilities for developing information system or application accreditation packages (i.e., security plan, security test and evaluation, etc.) in accordance with Departmental directives and applicable PCSPs.

*Training Evaluation Criteria:* **Demonstrate**

*Methods of Demonstration:* **Examination; Simulation; Desk Top Analysis**

*Level of Demonstration:*

**General** – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

**Functional** – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

**Detailed** – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **functional** knowledge of the DOE/PCSP and Operating Unit policies for identification of components comprising an information system and forms of accreditation
- Demonstrate a **detailed** ability to identify the constituent parts of a system and to apply controls based on those constituent parts
- Demonstrate a **detailed** ability to apply cyber security DOE/PCSP controls to systems and applications in the context of the Operating Unit mission environment

*Competency Area:* **System and Application Security**

*Functional Requirement:* **Implement**

*Competency Definition:* Refers to the knowledge of principles, practices, and procedures required to integrate information security into an Information Technology (IT) system or application during the System Development Life Cycle (SDLC). The goal of this activity is to ensure that the operation of IT systems and software does not present undue risk to the organization and information assets. Supporting activities include risk assessment, risk mitigation, security control selection, implementation and evaluation, certification and accreditation (C&A), and software security standards compliance.

*Behavioral Outcome:* The individual serving as an ISSO will understand the DOE C&A process and will implement and validate security controls required by the System Security Plan (SSP) as well as author/maintain C&A documentation as required by organizational policies.

*Training concepts to be addressed at a minimum (additional detailed training accomplished as required based on site-specific functional responsibilities):*

- Execute the C&A process to include determining the system categorization, identifying the minimum security controls and any additional security controls needed, implementing the security controls, and authoring the IT system or application System Security Plan (SSP).
- Execute configuration management practices as required by Departmental and/or PCSP policies and processes, the SSP, Configuration Management Plan (CMP), Contingency Plans, etc.
- Document POA&Ms as required for security controls that have not been implemented correctly.
- Document testing/validation results (i.e., findings and/or recommendations).
- Obtain information system or application accreditation or Interim Authorization to Operate (IATO) prior to going operational (i.e., processing live data).
- Implement and test backup and restore procedures for critical systems.

*Training Evaluation Criteria:* **Demonstrate**

*Methods of Demonstration:* **Examination; Simulation; Desk Top Analysis**

*Level of Demonstration:*

**General** – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

**Functional** – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

**Detailed** – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **functional** knowledge of the System Development Life Cycle
- Demonstrate a **functional** knowledge of certification and accreditation (C&A) processes
- Demonstrate a **detailed** knowledge of the SSP content requirement for the C&A process
- Demonstrate a **functional** knowledge of the approval required prior to production operation