DOE CYBERSECURITY:

CORE COMPETENCY TRAINING REQUIREMENTS

Key Cybersecurity Role: **Information System Security Manager (ISSM)**

Role Definition: The ISSM is the individual designated by an operating unit's (i.e., DOE organization or site) Senior Manager to manage the unit's cybersecurity program. This individual will be responsible for establishing, documenting, and monitoring the operating unit's cybersecurity program implementation as well as ensure unit compliance with the Senior DOE Risk Management Implementation Plan (RMIP). He/she must have a working knowledge of system functions, cybersecurity policies, and technical cybersecurity protection measures. Additionally, this individual will serve as the primary point of contact to the AO regarding all operating unit cybersecurity issues.

Competency Area: **Data Security**

Functional Requirement: **Manage**

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 the ISSM will have a working knowledge of the policies and procedures required to ensure the confidentiality, integrity, and availability of all categories of information and will apply this knowledge when establishing, implementing, and monitoring data security policies at the operating unit level.

Training concepts to be addressed at a minimum:

- Ensure that data classification and data management policies and guidance are issued and updated.
- Ensure compliance with data security policies and relevant legal and regulatory requirements in accordance with Departmental directives and applicable RMIP requirements.
- Ensure appropriate changes and improvement actions are implemented as required.
- Maintain current knowledge of authenticator management for unclassified and classified systems.
- Ensure compliance with protection requirements, control procedures, incident management reporting, remote access requirements, and system management for all systems as well as use of encryption for protecting Sensitive Unclassified Information (SUI) including Personally Identifiable Information (PII) and classified information.

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 existing data management policies within the organization
- Demonstrate a **detailed** knowledge of existing protection policies, requirements, and procedures
- Demonstrate a **detailed** ability to synthesize an Operating Unit cybersecurity management structure to implement DOE/Senior DOE Manager's (SDM) Program Cybersecurity Plan (PCSP) policies, requirements, and procedures and the information owner's protection requirements.
- Demonstrate a **detailed** knowledge of data access applications and system access control technologies.

Competency Area: **Data Security**

Functional Requirement: **Design**

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 the ISSM will have a working knowledge of the policies and procedures required to ensure the confidentiality, integrity, and availability of all categories of information and will apply this knowledge when establishing, implementing, and monitoring data security policies at the operating unit level.

Training concepts to be addressed at a minimum:

- Develop data security policies using data security standards, guidelines, and requirements that include privacy, authentication, access control, retention, disposal, incident management, disaster recovery, and configuration.
- Specify data and information classification, sensitivity, and need-to-know requirements by information type on a system in terms of its confidentiality, integrity, and availability. Utilize DOE M 205.1-5 to determine the information impacts for unclassified information and DOE M 205.1-4 to determine the Consequence of Loss for classified information.
- Develop acceptable use (e.g., personal use of IT policy; waste, fraud, and abuse policy, etc.) procedures in support of the data security policies.
- Develop sensitive data collection and management procedures in accordance with Departmental directives and applicable RMIP requirements.
- Develop media sanitization (clearing, purging, or destroying) and reuse procedures.
- Develop and document processes, procedures, and guidelines for complying with protection requirements (e.g., e-mail labels, media labels, etc.), control procedures (e.g., discretionary access control, need-to-know sharing, etc.), incident management reporting, remote access requirements, system management and use of encryption.
- Develop procedures for the release of non-system high information to systems accredited for

lower information sensitivities (classified or unclassified).

- Develop procedures for securing approval to release unclassified information to the public (DOE M 470.4-4, OPSEC).

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 DOE/RMIP policies, requirements, and procedures
- Demonstrate a **detailed** ability to synthesize Operating Unit data management policies and procedures based on the information owner's requirements and DOE/RMIP policies, requirements, and procedures.
- Demonstrate a **detailed** knowledge of sanitization methods and current equipment.

Competency Area: **Data Security**

Functional Requirement: **Evaluate**

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 the ISSM will have a working knowledge of the policies and procedures required to ensure the confidentiality, integrity, and availability of all categories of information and will apply this knowledge when establishing, implementing, and monitoring data security policies at the operating unit level.

Training concepts to be addressed at a minimum:

- Assess the effectiveness of data security policies, processes, and procedures against established Departmental directives and applicable PCSP requirements.
- Evaluate the effectiveness of the sensitivity determination processes by assessing unclassified non-SUI data at rest for OPSEC issues.
- Evaluate the effectiveness of solutions implemented to provide the required protection of data, including appropriate authenticator management and encryption controls.
- Review alleged violations of data security and privacy breaches.
- Identify improvement actions required to maintain the appropriate level of data protection.
- Evaluate the effectiveness of the media sanitization (clearing, purging, or destroying) and reuse processes.
- Evaluate the effectiveness of the processes and procedures for protecting SUI, including PII.

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 DOE/RMIP policies, requirements, and procedures
- Demonstrate a **detailed** knowledge of the types of information handled by the Operating Unit.
- Demonstrate a **detailed** ability to analyze protection implementations for compliance with stated requirements, policies, and procedures.
- Demonstrate a **functional** ability to develop assessment plans and procedures based on the types of information at the Operating Unit.
- Demonstrate a **detailed** knowledge of evaluation methodologies and the metrics they provide.
- Demonstrate a **detailed** ability to assess the effectiveness of protection measures as implemented.
- Demonstrate a **functional** knowledge of measurement techniques and methods
- Demonstrate a **detailed** knowledge of the use of metrics for evaluations

Competency Area: **Enterprise Continuity**

Functional Requirement: **Manage**

Competency Definition: Refers to application of the principles, policies, and procedures used to ensure that an organization continues to perform essential business functions within a defined accreditation boundary after the occurrence of a wide range of potential catastrophic events.

Behavioral Outcome: Individuals fulfilling the role of ISSM will have a working knowledge of the continuity of operations concepts to include disaster recovery, contingency plans, critical resource/facility continuity, delegation of authority, etc. He/she will apply this knowledge with establishing, implementing, and monitoring the operating unit's continuity of operations program.

Training concepts to be addressed at a minimum:

- Coordinate with stakeholders to establish the organizational continuity of operations program.
- Acquire necessary resources, including financial resources, to conduct an effective continuity of operations program.
- Define the continuity of operations organizational structure and staffing model.
- Define emergency delegations of authority and orders of succession for key positions.
- Define the scope of the continuity of operations program to address business continuity, business recovery, contingency planning, and disaster recovery related activities

- Ensure that each system is covered by a contingency plan.
- Integrate organizational concept of operations activities with related contingency planning activities.
- Define overall contingency objectives and criteria required for activating contingency plans.
- Establish a continuity of operations performance measurement program.
- Identify and prioritize critical business functions to include Critical Infrastructure and Key Resources.
- Ensure that appropriate changes and improvement actions are implemented as required.
- Apply lessons learned from test, training and exercise, and crisis events.

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 stakeholder operations and types of data
- Demonstrate a **functional** knowledge of the Operating Unit operations and programs with emergency/continuity of operations plans and the relationship of contingency planning for Information Technology.
- Demonstrate a **detailed** knowledge of contingency planning requirements.
- Demonstrate a **detailed** ability to analyze reports from tests and actual events and devise changes for Operating Unit enterprise continuity planning and operations.

Competency Area: **Incident Management**

Functional Requirement: **Manage**

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 Joint Cybersecurity Coordination Center (JC3).

Behavioral Outcome: Individuals fulfilling the role of ISSM will have a working knowledge of policies and procedures required to identify and respond to cybersecurity incidents, cybersecurity alerts, and INFOCON changes as directed by the JC3 and as mandated by organizational PCSP requirements. He/she will apply this knowledge when developing, implementing, and monitoring the Incident Response Management Plan and when coordinating incident response teams at the operating unit level.

Training concepts to be addressed at a minimum:

- Coordinate with stakeholders to establish the incident management program.

- Establish and coordinate activities of a Cybersecurity Incident Response Team (CIRT) to perform digital and network incident management activities.
- Establish relationships between the CIRT and internal individuals/groups (e.g., AO, classification officer, technical officer, Facility Security Officer, legal department, etc.) and external individuals and/or groups (e.g., JC3, law enforcement agencies, vendors, and public relations professionals).
- Acquire and manage resources, including financial resources, for incident management functions.
- Ensure users and incident management personnel are trained in incident reporting and handling procedures.
- Ensure coordination between the CIRT and the security administration and technical support teams.
- Provide adequate work space for the CIRT that at a minimum takes into account the electrical, thermal, acoustic, and privacy concerns (i.e., intellectual properties, classification, contraband) and security requirements (including access control and accountability) of equipment and personnel, and provide adequate report writing/administrative areas.
- Apply lessons learned from information security incidents to improve incident management processes and procedures.
- Ensure that appropriate changes and improvement actions are implemented as required.
- Maintain current knowledge on network forensic tools and processes.
- Establish an incident management measurement program.

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 DOE/RMIP incident response requirements and processes.
- Demonstrate a **detailed** knowledge of information types and incident types and categories.
- Demonstrate a **detailed** knowledge of the following organizations involvement with incidents
    - DOE JC3
    - Inspector General
    - Office of Intelligence and Counter-intelligence
    - Federal Bureau of Investigation
    - Local Law Enforcement
- Demonstrate a **detailed** knowledge of Operating Unit incident management processes.
- Demonstrate a **functional** knowledge of project planning principles and activities
- Demonstrate a **functional** knowledge of project tracking principles, activities, and methods
- Demonstrate a **detailed** knowledge of project management process and methods

- Demonstrate a **general** knowledge of physical facility space and capability requirements for office space, power, and networking connectivity requirements.
- Demonstrate a **functional** ability to provide policy and guidance for preservation of evidence, chain of custody, and processes to prevent loss/destruction of physical and electronic evidence.
- Demonstrate a **detailed** knowledge to interface INFOCON and incident management through operating Unit policy and guidance
- Demonstrate a **detailed** knowledge of forensics capabilities available for use during cybersecurity incident investigation

Competency Area: **Incident Management**

Functional Requirement: **Design**

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 Joint Cybersecurity Coordination Center (JC3).

Behavioral Outcome: Individuals fulfilling the role of ISSM will have a working knowledge of policies and procedures required to identify and respond to cybersecurity incidents, cybersecurity alerts, and INFOCON changes as directed by the JC3 and as mandated by organizational PCSP requirements. He/she will apply this knowledge when developing, implementing, and monitoring the Incident Response Management Plan and when coordinating incident response teams at the operating unit level.

Training concepts to be addressed at a minimum:

- Create an Incident Response Management Plan, to include impact assessments and incident categorization requirements, in accordance with Departmental directives and applicable PCSP requirements.
- Develop procedures for reporting INFOCON changes and security incidents, including confirmed or potential incidents involving Personally Identifiable Information (PII), to JC3.
- Identify services that the incident response team should provide.
- Develop procedures for performing incident and INFOCON responses and maintaining records.
- Develop procedures for handling information and cyber alerts disseminated by the DOE JC3.
- Create incident response exercises and penetration testing activities.
- Specify incident response staffing and training requirements to include general users, system administrators, and other affected personnel.
- Establish an incident management measurement program.
- Develop policies for preservation of electronic evidence, data recovery and analysis, and the reporting and archival requirements of examined material in accordance with procedures set forth by the DOE JC3.
- Adopt or create chain of custody procedures that include disposal procedures and, when required, the return of media to its original owner in accordance with procedures set forth by the DOE JC3.

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 DOE/RMIP incident response requirements and processes.
- Demonstrate a **detailed** knowledge of the following organizations involvement with incidents
    - DOE JC3
    - Inspector General
    - Office of Intelligence and Counter-intelligence
    - Federal Bureau of Investigation
    - Local Law Enforcement
- Demonstrate a **detailed** ability to analyze DOE/RMIP requirements to devise a plan to implement and support incident detection, handling, and reporting.
- Demonstrate a **functional** knowledge of exercising and testing incident response and system/network vulnerabilities.
- Demonstrate a **functional** knowledge of performance measurement techniques and methods
- Demonstrate a **detailed** knowledge of the use of metrics for evaluations

Competency Area: **Cybersecurity Training and Awareness**

Functional Requirement: **Manage**

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 the ISSM will understand the concepts of effective cybersecurity awareness activities to influence human behavior as well as understand the criticality of regular cybersecurity training for individuals with information security roles. He/she will apply this knowledge when establishing, implementing, and monitoring the Cybersecurity Awareness and Training (CSAT) Program at the operating unit level.

Training concepts to be addressed at a minimum:

- Identify business requirements and establish organizational policy for the cybersecurity awareness and training program that complies with Departmental directives and applicable PCSP requirements.
- Acquire and manage necessary resources, including financial resources, to support the cybersecurity awareness and training program.
- Set operational performance measures for training and delivery and assess compliance with such performance measures.

- Ensure that appropriate changes and improvement actions are implemented 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 **detailed** knowledge of DOE/RMIP training policy, standards, and guidance.
- Demonstrate a **functional** knowledge of training methodologies
- Demonstrate a **functional** ability to identify cybersecurity training as it relates to Operating Unit missions and information
- Demonstrate a **functional** knowledge of training evaluation techniques and methods
- Demonstrate a **functional** knowledge of measurement techniques and methods

Competency Area: **Cybersecurity Training and Awareness**

Functional Requirement: **Design**

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 the ISSM will understand the concepts of effective cybersecurity awareness activities to influence human behavior as well as understand the criticality of regular cybersecurity training for individuals with information security roles. He/she will apply this knowledge when establishing, implementing, and monitoring the Cybersecurity Awareness and Training (CSAT) Program at the operating unit level.

Training concepts to be addressed at a minimum:

- Develop a workforce development, training, and awareness program plan in accordance with Departmental directives and applicable PCSPs.
- Define the goals and objectives of the operating unit's cybersecurity awareness and training program.
- Work with appropriate security SMEs to ensure completeness and accuracy of the security training and awareness program.
- Establish a tracking and reporting process for the cybersecurity training and awareness program.
- Ensure currency and accuracy of training and awareness materials.

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 DOE/RMIP training policy, standards, and guidance
- Demonstrate a **functional** knowledge of project planning principles and activities
- Demonstrate a **functional** knowledge of project tracking principles, activities, and methods
- Demonstrate a **detailed** ability to prepare documentation to describe the implementing requirements for DOE/RMIP training policy
- Demonstrate a **functional** knowledge of current to threat, technology, and vulnerability changes to address changes/updates for training and awareness

Competency Area: **Cybersecurity 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 the ISSM will understand the concepts of effective cybersecurity awareness activities to influence human behavior as well as understand the criticality of regular cybersecurity training for individuals with information security roles. He/she will apply this knowledge when establishing, implementing, and monitoring the Cybersecurity Awareness and Training (CSAT) Program at the operating unit level.

Training concepts to be addressed at a minimum in course curricula:

- Perform a needs assessment to determine skill gaps and identify personnel in roles requiring training based on mission requirements in accordance with Departmental directives and applicable PCSPs.
- Develop new or identify existing awareness and training materials that are appropriate and timely for intended audiences.
- Communicate management's commitment, and the importance of the cybersecurity awareness and training program, to the workforce.

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 DOE/RMIP roles and responsibilities
- Demonstrate a **detailed** knowledge of public law, regulations, and Operating Unit training policy, standards, and guidance.
- Demonstrate a **functional** knowledge of training and awareness methodologies that can be used to provide effective training.
- Demonstrate a **functional** ability to prepare lesson plan outlines and topics to guide training and awareness presentation
- Demonstrate a **detailed** ability to present an overview of the RMIP and Operating Unit implementation to show management's commitment.

Competency Area: **Cybersecurity Training and Awareness**

Functional Requirement: **Evaluate**

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 the ISSM will understand the concepts of effective cybersecurity awareness activities to influence human behavior as well as understand the criticality of regular cybersecurity training for individuals with information security roles. He/she will apply this knowledge when establishing, implementing, and monitoring the Cybersecurity Awareness and Training (CSAT) Program at the operating unit level.

Training concepts to be addressed at a minimum in course curricula:

- Assess and evaluate the cybersecurity awareness and training program for compliance with Departmental directives and applicable PCSPs; initiate improvements where needed.
- Assess the awareness and training program to ensure that it meets not only the organization's stakeholder needs, but that it effectively covers current cybersecurity issues and legal requirements.
- Ensure that information security personnel are receiving the appropriate level and type of training.

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 DOE/RMIP roles and responsibilities
- Demonstrate a **functional** ability to analyze and compare standards , guidelines, policies, and processes
- Demonstrate a **detailed** ability to analyze policy, law, and regulation implementations to determine appropriateness and coverage of the implementation
- Demonstrate a **detailed** ability to analyze training information to determine appropriateness of training content based on the role
- Demonstrate a **functional** knowledge of methodologies that can be used to determine the effectiveness of training
- Demonstrate a **functional** knowledge of project planning principles and activities
- Demonstrate a **functional** knowledge of project tracking principles, activities, and methods
- Demonstrate a **detailed** ability to prepare documentation to describe the assessment methods and expected results for training and awareness

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

Functional Requirement: **Manage**

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 the ISSM will have a working knowledge of the policies, procedures, and controls required to protect IT infrastructure and data to include technical, operational, and administrative security controls and will apply this knowledge when establishing, implementing, and monitoring the IT infrastructure security administration program at the operating unit level.

Training concepts to be addressed at a minimum:

- Establish IT infrastructure security administration program scope, goals and objectives in accordance with Departmental directives and applicable PCSPs.
- Monitor the IT infrastructure security administration program budget.
- Direct security administration personnel to include individuals with cybersecurity key roles.
- Identify and manage IT infrastructure security administration program risks.
- Establish communications between the security administration team and other security-related personnel (e.g., technical support, incident management, etc.).

- Integrate security administration team activities with other security-related team activities (e.g., technical support, incident management, security engineering, etc.).
- Acquire necessary resources, including financial resources, to execute the IT infrastructure security administration program.

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 DOE/RMIP policy, standards, and guidance
- Demonstrate a **functional** knowledge of the Operating Unit budgeting process
- Demonstrate a **functional** knowledge of personnel management policy, activities, and procedures
- Demonstrate a **functional** knowledge of other security disciplines that impact cybersecurity
- Demonstrate a **functional** ability to identify and manage interfaces with other security functions and mission implementation functions

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

Functional Requirement: **Design**

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 the ISSM will have a working knowledge of the policies, procedures, and controls required to protect IT infrastructure and data to include technical, operational, and administrative security controls and will apply this knowledge when establishing, implementing, and monitoring the IT infrastructure security administration program at the operating unit level.

Training concepts to be addressed at a minimum:

- Develop IT infrastructure security administration processes and procedures in accordance with Departmental directives and applicable PCSP requirements.
- Develop vulnerability and patch management process.

- Develop security administration change management procedures to ensure that security policies and controls remain effective following a change to include identification of roles and responsibilities for change approval and/or disapproval.
- Define information technology security performance measures.
- Develop a continuous monitoring and analysis process that includes configuration management; security control monitoring through reviews and assessments of the system and its operational, logical, and physical environment; and status reporting and documentation maintenance.

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 DOE/RMIP policy, standards, and guidance
- Demonstrate a **functional** knowledge of test methodologies, processes, and reporting
- Demonstrate a **functional** knowledge of configuration management and control principles and processes
- Demonstrate a **functional** knowledge of evaluation methodologies, processes, and reporting
- Demonstrate a **functional** knowledge of methods and technologies to provide capabilities for monitoring and reporting on network/system operation and vulnerabilities
- Demonstrate a **detailed** knowledge of points for obtaining metrics for cybersecurity
- Demonstrate a **detailed** ability to structure performance by meaningful measures

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

Functional Requirement: **Evaluate**

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 the ISSM will have a working knowledge of the policies, procedures, and controls required to protect IT infrastructure and data to include technical, operational, and administrative security controls and will apply this knowledge when establishing, implementing, and monitoring the IT infrastructure security administration program at the operating unit level.

Training concepts to be addressed at a minimum:

- Review strategic IT infrastructure security technologies that meet operating unit goals and mission.
- Review performance and correctness of applied security controls in accordance with Departmental directives and applicable PCSP requirements.
- Assess the performance of IT infrastructure security administration measurement technologies.
- Assess the effectiveness of the patch and vulnerability management processes.
- Identify improvement actions through a Plan of Action and Milestones (POA&M) based on reviews, assessments, and other data sources.

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 DOE/RMIP policy, standards, and guidance
- Demonstrate a **detailed** ability to analyze the implementation of controls and propose changes in implementation
- Demonstrate a **detailed** ability to analyze control implementation to determine compliance with DOE/RMIP data security policies, processes, procedures, directives, regulations, and public laws (statutes)
- Demonstrate a **functional** knowledge of security technologies available for demonstrating and measuring control implementations
- Demonstrate a **functional** knowledge of the purpose of POA&Ms and the procedures for creating and coordinating a POA&M

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

Functional Requirement: **Manage**

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 the ISSM will have a working knowledge of the policies, procedures, and controls required to protect network and telecommunication services to include technical, operational, and administrative security controls. He/she will apply this knowledge when establishing, implementing, and monitoring the network and telecommunications security program at the operating unit level.

Training concepts to be addressed at a minimum:

- Collaborate with responsible organizations to establish a network and telecommunications security program in accordance with Departmental directives and applicable PCSP requirements.
- Establish communications between the network and telecommunications security team and related security teams (e.g., technical support, cybersecurity administration, incident response, etc.).
- Ensure the development of a risk-based approach for implementing system interconnections and wireless technologies.
- Ensure policies and processes governing the conditions under which remote access can be granted and terminated are developed.
- Ensure the establishment of a management review process that addresses network-based and remote access audits and allows for timely process improvements.
- Establish specific training and support requirements for External Information Systems and portable/mobile devices including protection of government information, secure operation, implementation of minimum security controls, individual rules of behavior, and consequences for rule violation.
- Ensure the use and management of Peer-to-Peer (P2P) networking is defined and documented 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 **detailed** knowledge of DOE/RMIP data security policy, standards, and guidance and public law
- Demonstrate a **detailed** knowledge of network and telecommunication policies, procedures, and controls and the implementation of technologies used for the interconnection of systems/networks via wired or wireless access, remote access, P2P, and the utilization of external systems
- Demonstrate a **functional** knowledge of the vulnerabilities, issues, and threats that are related to the use of various networking technologies and the interconnection of networks/systems/ components
- Demonstrate a **detailed** ability to determine the effectiveness of network, external system, and remote user training
- Demonstrate a **functional** knowledge of other security disciplines that impact cybersecurity
- Demonstrate a **functional** knowledge of training approaches and methods of delivery

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

Functional Requirement: **Design**

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 the ISSM will have a working knowledge of the policies, procedures, and controls required to protect network and telecommunication services to include technical, operational, and administrative security controls. He/she will apply this knowledge when establishing, implementing, and monitoring the network and telecommunications security program at the operating unit level.

Training concepts to be addressed at a minimum:

- Develop network and host-based security policies in accordance with Departmental directives and applicable PCSP requirements.
- Establish processes and procedures for protecting telecommunications networks against unauthorized access and wiretapping (e.g., protected distribution systems, transmission encryption, locked telephone closets, etc.).
- Establish processes and procedures for mitigating the loss of confidentiality of SUI or classified information in coordination with applicable security organizations/disciplines to include TEMPEST, emanations, and Technical Surveillance Countermeasures (TSCM).
- Develop process for interconnecting information systems based on identifying organizational needs, associated risks, and controlled interface requirements.
- Ensure the development of effective network domain security controls in accordance with organizational, network, and host-based policies.
- Develop network security performance reports.
- Develop network security and telecommunication audit processes, guidelines, and procedures.
- Develop wireless technology processes, guidelines, and procedures in accordance with Departmental directives and applicable PCSPs
- Develop and document processes, procedures, and guidelines related to P2P networking commensurate with the level of security required for the organization's environment and specific needs *and* in accordance with Departmental directives and applicable PCSPs.
- Develop processes, procedures, and identify minimum security controls for External Information Systems and portable/mobile devices.

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 DOE/RMIP data security policy, standards, and guidance, and public law
- Demonstrate a **functional** knowledge of project management principles and activities
- Demonstrate a **functional** knowledge of other security disciplines that impact cybersecurity
- Demonstrate a **functional** ability to identify and manage interfaces with other security functions and mission implementation functions
- Demonstrate a **detailed** knowledge of technical report writing
- Demonstrate a **detailed** ability to analyze policy, control statements, standards, guidance, and regulations for the development of procedures and control implementations
- Demonstrate a **detailed** knowledge of threats and vulnerabilities to evaluate the potential impact and related risk to an Operating Unit infrastructure and individual systems
- Demonstrate a **detailed** ability to evaluate the applicability of threats and vulnerabilities to networks/information systems
-

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

Functional Requirement: **Evaluate**

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 the ISSM will have a working knowledge of the policies, procedures, and controls required to protect network and telecommunication services to include technical, operational, and administrative security controls. He/she will apply this knowledge when establishing, implementing, and monitoring the network and telecommunications security program at the operating unit level.

Training concepts to be addressed at a minimum:

- Evaluate the effectiveness of implemented network protection policies, procedures, as well as minimum security controls for portable/mobile devices, External Information Systems, wireless technologies, and P2P network capabilities for compliance with Departmental directives and applicable PCSP requirements.
- Ensure that interconnected systems do not adversely affect the confidentiality, integrity, or availability of the connected systems.
- Ensure that remote access polices are being effectively implemented and that affected users are knowledgeable of information security requirements when processing DOE information off site
- Ensure that appropriate solutions to eliminate or otherwise mitigate identified vulnerabilities are implemented effectively.
- Assess adequacy of functional security requirements by arranging independent verification and validation testing activities for networks as required.
- Ensure that anti-malware systems are effective via self assessment reports, performance measures, certification testing, etc.

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 DOE/RMIP data security policy, standards, and guidance, and public law
- Demonstrate a **detailed** knowledge of network and telecommunication policies, procedures, and controls and the implementation of technologies used for the interconnection of systems/networks via wired or wireless access, remote access, P2P, and the utilization of external systems
- Demonstrate a **functional** knowledge of the vulnerabilities, issues, and threats that are related to the use of various networking technologies and the interconnection of networks/systems/ components
- Demonstrate a **detailed** ability to determine the effectiveness of network, external system, and remote user training
- Demonstrate a **detailed** ability to analyze procedures and control implementations for effectiveness and compliance with policy, control statements, standards, guidance, and regulations
- Demonstrate a **detailed** ability to analyze Operating Unit policies for effectiveness and compliance with DOE/RMIP policy, standards, and guidance

Competency Area: **Personnel Security**

Functional Requirement: **Manage**

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 the ISSM will have a working knowledgeable of Personnel Security policies and procedures and will coordinate with the appropriate security offices to ensure that personnel security access controls are implemented as required by system functional design specifications and as mandated by Departmental directives and applicable PCSP standards.

Training concepts to be addressed at a minimum:

- Coordinate with Physical Security, Operations Security (OPSEC), and other organizational managers to ensure a coherent, coordinated, and holistic approach to security across the operating unit.

- Ensure personnel security compliance with Departmental directives and applicable PCSP requirements via periodic self-assessments, program reviews, and system certification testing activities.
- Recommend the implementation of appropriate changes and improvement actions 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 **general** knowledge of DOE/RMIP personnel security policy, standards, and guidance, and regulations
- Demonstrate a **functional** knowledge of other security disciplines and their interface with cybersecurity
- Demonstrate a **functional** ability to analyze other security discipline implementations for effectiveness and compliance with RMIP and Operating Unit cybersecurity policies and control statements
- Demonstrate the **functional** ability to develop change recommendations to improve the effectiveness of personnel cybersecurity control implementations

Competency Area: **Personnel Security**

Functional Requirement: **Design**

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 the ISSM will have a working knowledgeable of Personnel Security policies and procedures and will coordinate with the appropriate security offices to ensure that personnel security access controls are implemented as required by system functional design specifications and as mandated by Departmental directives and applicable PCSP standards.

Training concepts to be addressed at a minimum in course curricula:

- Establish personnel security processes and procedures for individual job roles to include key cybersecurity roles.
- Establish procedures for coordinating with other organizations to ensure that common processes (e.g., management authorizations) are aligned and not duplicated.
- Establish personnel security rules and procedures to which external suppliers (e.g.,

vendors, contractors, etc.) must conform.

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 DOE/RMIP personnel and cybersecurity policy, standards, and guidance, and regulations
- Demonstrate a **functional** ability to determine information sensitivity for information used/created by external suppliers
- Demonstrate a **functional** ability to analyze policy, standards and regulations in combination with control statements to develop personnel security procedures each identified role

Competency Area: **Physical and Environmental Security**

Functional Requirement: **Manage**

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 to 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 the ISSM will have a working knowledgeable of Physical Security policies and procedures and will coordinate with the appropriate security offices to ensure that physical controls are implemented as required by the system functional design specifications, as required to adequately protect computing facilities and equipment form natural or man-made threats, and as mandated by Departmental directives and applicable PCSP standards.

Training concepts to be addressed at a minimum:

- Coordinate with personnel managing IT infrastructure security, Personnel Security, COMSEC, Operations Security, and other security functional areas to provide an integrated, holistic, and coherent security effort.
- Ensure physical security compliance with Departmental directives and applicable PCSP requirements via periodic self-assessments, program reviews, and system certification testing activities.
- Recommend the implementation of appropriate changes and improvement actions 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 **general** knowledge of DOE/RMIP physical and cybersecurity policy, standards, and guidance, and regulations
- Demonstrate a **functional** knowledge of cybersecurity interactions/interfaces with other security disciplines
- Demonstrate a **functional** ability to determine physical security implementations of cybersecurity controls
- Demonstrate a **functional** ability to analyze policy, standards and regulations in combination with control statements to recommend changes to physical security procedures

Competency Area: **Physical and Environmental Security**

Functional Requirement: **Design**

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 to 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 the ISSM will have a working knowledgeable of Physical Security policies and procedures and will coordinate with the appropriate security offices to ensure that physical controls are implemented as required by the system functional design specifications, as required to adequately protect computing facilities and equipment form natural or man-made threats, and as mandated by Departmental directives and applicable PCSP standards.

Training concepts to be addressed at a minimum:

- Identify physical security program requirements and specifications in relationship to system security goals.
- Develop policies and procedures for identifying and mitigating physical and environmental threats (to include TEMPEST concerns) to information assets, personnel, facilities, and equipment.
- Develop a physical security and environmental security plan, including security test plans and contingency plans, in coordination with other security planning functions as required by Departmental directives and applicable PCSPs.
- Recommend cybersecurity criteria to be included in acquisition specifications for facilities, equipment, and services.

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 DOE/RMIP physical security policy, standards, and guidance and regulations
- Demonstrate a **functional** ability to analyze cybersecurity controls and physical security policy to identify common controls for information systems
- Demonstrate a **general** knowledge of procurement processes sufficient to identify cybersecurity requirements in appropriate format for procurements
- Demonstrate a **general** knowledge of methods for mitigating physical proximity threats for system components, personnel, and facilities.

Competency Area: **Regulatory and Standards Compliance**

Functional Requirement: **Manage**

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 the ISSM will understand the policies and procedures required for an operating unit to comply with applicable information security laws, regulations, Departmental policy, and industry-wide best practices. He/she will apply this knowledge when establishing, implementing, monitoring, and communicating the unit's information security compliance strategies, policies, and procedures.

Training concepts to be addressed at a minimum:

- Establish and administer a risk-based information security program that complies with Departmental directives and applicable PCSP requirements.
- Define the operating unit's information security compliance/assessment program to include the development, management, and reporting of POA&Ms.
- Coordinate and provide liaison with staffs that are responsible for information security compliance, licensing and registration, and data security surveillance.
- Collaborate with organizations responsible for the development and implementation of Privacy Impact Assessments.
- Identify and stay current on all external laws, regulations, standards, and best practices

applicable to the operating unit.

- Identify major risk factors (product, compliance, and operational) and coordinate the application of information security strategies, plans, policies, and procedures to reduce regulatory risk.
- Maintain relationships with regulatory information security organizations and appropriate industry groups, forums, and stakeholders.
- Keep informed on pending information security changes, trends, and best practices by participating in collaborative settings.
- Acquire the necessary resources to support an effective information security compliance/self-assessment program
- Utilize lessons learned from compliance activities to implement appropriate changes and improvement actions 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 **detailed** knowledge of public law, regulations, and DOE/PCSP/RMF and Operating Unit policy, standards, and guidance
- Demonstrate a **detailed** ability to communicate program objectives and implementation to Operating Unit Management and staff
- Demonstrate a **detailed** ability to accomplish project management activities such as scheduling, assigning tasks, and managing funding
- Demonstrate a **functional** knowledge of government and industry organizations involved in cybersecurity and their areas of expertise
- Demonstrate a **functional** knowledge of the Operating Unit budgeting and personnel staffing processes

Competency Area: **Regulatory and Standards Compliance**

Functional Requirement: **Design**

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 the ISSM will understand the policies and procedures required for an operating unit to comply with applicable information security laws, regulations, Departmental policy, and industry-wide best practices. He/she will apply this knowledge when establishing, implementing, monitoring, and communicating the unit's information security compliance

strategies, policies, and procedures.

Training concepts to be addressed at a minimum:

- Develop information security compliance strategies, policies, plans, and procedures in accordance with Departmental directives and applicable PCSP requirements.
- Specify information security compliance program control requirements.
- Develop an information security compliance performance measurement program.
- Develop a process for documenting system-level and program-level deficiencies and associated mitigation strategies in POA&Ms as identified during compliance and/or self-assessment activities.

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 public law, regulations, and DOE/PCSP/RMF and Operating Unit policy, standards, and guidance
- Demonstrate a **functional** knowledge of program management sufficient to provide a framework for project management, budget formulation, program direction, implementation strategies, plans, and procedures.
- Demonstrate a **detailed** knowledge of methodologies including self-assessments, surveys, site assistance visits, etc. for ensuring compliance with program requirements
- Demonstrate a **detailed** knowledge of methodologies for determining compliance with program objectives and schedules

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 the ISSM will understand the policies and procedures required for an operating unit to comply with applicable information security laws, regulations, Departmental policy, and industry-wide best practices. He/she will apply this knowledge when establishing, implementing, monitoring, and communicating the unit's information security compliance strategies, policies, and procedures.

Training concepts to be addressed at a minimum:

- 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 POA&Ms 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 **detailed** knowledge of public law, regulations, and DOE/PCSP/RMF and Operating Unit policy, standards, and guidance
- Demonstrate a **functional** knowledge of program management sufficient to provide a framework for project management, budget formulation, program direction, implementation strategies, plans, and procedures.
- Demonstrate a **detailed** knowledge of methodologies including self-assessments, surveys, site assistance visits, etc. for ensuring compliance with program requirements
- Demonstrate a **detailed** ability to develop adequate tests and evaluation measures to determine control effectiveness
- Demonstrate a **detailed** ability to analyze practices for compliance with DOE policy and procedures
- Demonstrate a **detailed** knowledge to develop novel control implementations to mitigate implementation deficiencies

Competency Area: **Regulatory and Standards Compliance**

Functional Requirement: **Evaluate**

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 the ISSM will understand the policies and procedures required for an operating unit to comply with applicable information security laws, regulations,

Departmental policy, and industry-wide best practices. He/she will apply this knowledge when establishing, implementing, monitoring, and communicating the unit's information security compliance strategies, policies, and procedures.

Training concepts to be addressed at a minimum:

- Monitor, assess, and report information security compliance practices for information systems in accordance with Departmental directives and applicable PCSP requirements; implement changes where 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 **detailed** knowledge of public law, regulations, and DOE/PCSP/RMF and Operating Unit policy, standards, and guidance
- Demonstrate a **detailed** knowledge of assessment methods and techniques
- Demonstrate a **detailed** knowledge of practices for determining compliance with policy and procedures
- Demonstrate a **detailed** ability to perform analyses of Senior DOE Management implementation of Departmental standards, policies, procedures, guidelines, directives, and regulations and laws (statutes)
- Demonstrate a **detailed** ability to analyze practices for compliance with DOE policy and procedures
- Demonstrate a **functional** knowledge of assessment reporting processes and procedures
- Demonstrate a **detailed** knowledge of evaluation methodologies and the metrics they provide.

Competency Area: **Security Risk Management**

Functional Requirement: **Manage**

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 the ISSM will have a working knowledgeable of Departmental risk management policies, procedures, and mitigation strategies and will apply this knowledge when establishing, implementing, and monitoring the risk management program at the operating unit level.

Training concepts to be addressed at a minimum:

- Establish a threat-based risk management program based on organizational/operating unit missions, business goals, and objectives and in accordance with Departmental directives and applicable PCSP requirements.
- Ensure the impact of security risks on mission, business goals, objectives, plans, programs, and actions are presented to the AO during the accreditation decision making process.
- Acquire and manage the resources, including financial resources, necessary to implement an effective risk management program.
- Ensure that appropriate changes and improvement actions as identified during risk analysis activities are implemented as required.
- Ensure that the equivalency/exemption process is in place and functional

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 Departmental/PCSP policies and procedures for evaluating and managing risk to Operating Unit operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation
- Demonstrate a **functional** knowledge of threats and threat sources
- Demonstrate a **functional** knowledge of Operating Unit missions and site/facility assignment of missions
- Demonstrate a **functional** knowledge of program management sufficient to provide a framework for project management, budget formulation, program direction, implementation strategies, plans, and procedures.
- Demonstrate a **functional** ability to analyze security risk assessments based on operating Unit missions and business goals and objectives

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 the ISSM will have a working knowledgeable of Departmental risk management policies, procedures, and mitigation strategies and will apply this knowledge when establishing, implementing, and monitoring the risk management program at the

operating unit level.

Training concepts to be addressed at a minimum:

- Develop and maintain risk-based security policies, plans, and procedures based on Departmental directives and applicable PCSP requirements.
- Ensure that the risk assessment process provides for identifying and assessing environmental (i.e., operational, logical, or physical) and system risks to information assets, personnel, facilities, and equipment and mitigating such risks.
- Develop processes and procedures for determining the costs and benefits of risk mitigation strategies.
- Develop procedures for documenting the decision to apply mitigation strategies or acceptance of risk.

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 Departmental/PCSP policies and procedures for evaluating and managing risk to Operating Unit operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation
- Demonstrate a **functional** knowledge of methodologies and techniques for evaluating risks
- Demonstrate a **functional** knowledge of risk management techniques
- Demonstrate a **detailed** ability to identify applicability of risk management techniques
- Demonstrate a **detailed** knowledge of potential changes in configuration that may impact security function/control effectiveness
- Demonstrate a **functional** knowledge of costs associated with security implementation
- Demonstrate a **functional** knowledge of methods of control implementations and the associated risks
- Demonstrate a **detailed** ability to analyze DOE/PCSP policies and procedures for evaluating and managing risk to Operating Unit operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation and identify methods, processes, and steps to implement them

Competency Area: **Security Risk Management**

Functional Requirement: **Evaluate**

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 the ISSM will have a working knowledgeable of Departmental risk management policies, procedures, and mitigation strategies and will apply this knowledge when establishing, implementing, and monitoring the risk management program at the operating unit level.

Training concepts to be addressed at a minimum:

- Assess the effectiveness of the risk management program against Departmental directives and applicable PCSP requirements and implement changes where required.
- Review the performance of risk management tools and techniques.
- Assess results of threat and vulnerability assessments to identify security risks and regularly update applicable security controls.
- Make determination on acceptance of residual risk as permitted by Departmental directives and applicable PCSPs.
- Identify changes to risk management policies and processes that will enable them to remain current with the emerging risk and threat environment.

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 DOE/PCSP/Operating Unit policies, processes, procedures, directives, regulations, and public laws (statutes)
- Demonstrate a **detailed** knowledge of the DOE/PCSP 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 of DOE/PCSP risk management framework
- Demonstrate a **functional** ability to analyze DOE/PCSP description of the risk management framework and devise implementation concepts for the Operating Unit
- Demonstrate a **functional** knowledge of risk management techniques
- Demonstrate a **detailed** ability to identify applicability of risk management techniques
- Demonstrate a **detailed** ability to analyze vulnerabilities and threats to determine the likelihood of successful attack and resulting impacts
- Demonstrate a **functional** knowledge of methodologies and techniques for evaluating the effectiveness of risk management policies, processes, and procedures
- Demonstrate a **detailed** knowledge of technologies used within the Operating Unit and current technologies to identify new controls or implementations of controls

Competency Area: **Strategic Security Management**

Functional Requirement: **Manage**

Competency Definition: Refers to the knowledge of principles, practices, and methods involved in making managerial decisions and actions that determine the long-term performance of an organization. The goal of strategic security management is to ensure that an organization's security practices and policies are in line with the mission statement.

Behavioral Outcome: The individual serving as the ISSM will be knowledgeable of Departmental cybersecurity policies, strategic direction, mission objectives, infrastructure initiatives, and security funding priorities. He/she will apply this knowledge when establishing, implementing, monitoring, and communicating cybersecurity policies and strategic planning initiatives at the operating unit level.

Training concepts to be addressed at a minimum:

- Establish cybersecurity program goals that are in accordance with Departmental directives and applicable PCSP requirements.
- Establish a cybersecurity program to provide security for all systems, networks, and data that support the operations and business/mission needs of the organization/operating unit.
- Integrate and align cybersecurity, physical security, personnel security, and other security components into a systematic process to ensure that information protection goals and objectives are reached.
- Align cybersecurity priorities with the operating unit's mission and vision and communicate the value of cybersecurity within the organization.
- Coordinate all aspects of the cybersecurity program at the operating unit level with Senior DOE Management.
- Acquire and manage the necessary resources, including financial resources, to support cybersecurity goals and objectives and reduce overall risk.
- Establish overall architecture goals by aligning business processes, software and hardware, local and wide area networks, people, operations, and projects with the overall security strategy and the Department's Enterprise Architecture strategy.

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 DOE/PCSP/Operating Unit policies, processes, procedures, directives, regulations, and public laws (statutes)
- Demonstrate a **functional** knowledge of the Operating Unit mission(s) and mission criticalities

- Demonstrate a **functional** knowledge of the Senior DOE Management and Operating Unit mission and business goals and objectives
- Demonstrate a **functional** knowledge of the DOE, Senior DOE Management, and Operating Unit Enterprise Architecture(s)
- Demonstrate a **functional** knowledge of technical architecture design as it relates to the implementation of an Enterprise Architecture
- Demonstrate a **functional** knowledge of physical, personnel, and other security disciplines
- Demonstrate a **functional** knowledge of capital planning and investment control and the impacts to cybersecurity
- Demonstrate a **detailed** ability to perform analyses to prioritize security policy and processes relative to mission accomplishment and business functions
- Demonstrate a **detailed** ability to establish cybersecurity goals based on DOE/PCSP/Operating Unit policies, processes, procedures, directives, regulations, and public laws (statutes); Operating Unit mission; Operating Unit investment portfolio; and Departmental and Operating Unit Enterprise Architecture

Competency Area: **Strategic Security Management**

Functional Requirement: **Design**

Competency Definition: Refers to the knowledge of principles, practices, and methods involved in making managerial decisions and actions that determine the long-term performance of an organization. The goal of strategic security management is to ensure that an organization's security practices and policies are in line with the mission statement.

Behavioral Outcome: The individual serving as the ISSM will be knowledgeable of Departmental cybersecurity policies, strategic direction, mission objectives, infrastructure initiatives, and security funding priorities. He/she will apply this knowledge when establishing, implementing, monitoring, and communicating cybersecurity policies and strategic planning initiatives at the operating unit level.

Training concepts to be addressed at a minimum:

- Establish a performance management program that will measure the efficiency, effectiveness, and maturity of the cybersecurity program in support of the operating unit's business and mission needs/goals.
- Develop information security management strategic plans.
- Integrate applicable laws and regulations into information security strategy, plans, policies, and procedures.

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 DOE/PCSP/Operating Unit policies, processes, procedures, directives, regulations, and public laws (statutes)
- Demonstrate a **functional** knowledge of Senior DOE Management methods and techniques to measure performance of the Operating Unit cybersecurity activities in conjunction with Operating Unit missions and business needs
- Demonstrate a **detailed** ability to integrate cybersecurity with mission and business needs to provide strategic direction for the Operating Unit cybersecurity program
- Demonstrate a **detailed** ability to provide comprehensive, logical documentation of strategic planning efforts

Competency Area: **Strategic Security Management**

Functional Requirement: **Implement**

Competency Definition: Refers to the knowledge of principles, practices, and methods involved in making managerial decisions and actions that determine the long-term performance of an organization. The goal of strategic security management is to ensure that an organization's security practices and policies are in line with the mission statement.

Behavioral Outcome: The individual serving as the ISSM will be knowledgeable of Departmental cybersecurity policies, strategic direction, mission objectives, infrastructure initiatives, and security funding priorities. He/she will apply this knowledge when establishing, implementing, monitoring, and communicating cybersecurity policies and strategic planning initiatives at the operating unit level.

Training concepts to be addressed at a minimum:

- Provide feedback to management and the AO on the effectiveness and performance of security strategic plans in accomplishing business/mission needs.
- Perform internal and external analyses to ensure cybersecurity policies and practices are in line with the operating unit's mission.
- Integrate business goals with information security program policies, plans, processes, and procedures.
- Collect, analyze, and report performance measures.
- Use performance measures to enhance strategic decision making.

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 DOE/PCSP/Operating Unit policies, processes, procedures, directives, regulations, and public laws (statutes)
- Demonstrate a **functional** ability to provide methods to measure the accomplishment of cybersecurity goals to assist in accomplishing DOE/PCSP policies, processes, procedures, directives, regulations, and public laws (statutes); organization mission; investment portfolio costs; and Departmental and organizational Enterprise Architecture functions
- Demonstrate a **functional** ability to perform analyses of organizational missions and goals in order to apply appropriate cybersecurity principles to formulate cybersecurity policies and processes
- Demonstrate a **detailed** knowledge of evaluation methodologies and the metrics they provide.
- Demonstrate a **detailed** ability to assess the effectiveness of protection measures as implemented.
- Demonstrate a **functional** knowledge of measurement techniques and methods
- Demonstrate a **detailed** knowledge of the use of metrics for evaluations

Competency Area: **Strategic Security Management**

Functional Requirement: **Evaluate**

Competency Definition: Refers to the knowledge of principles, practices, and methods involved in making managerial decisions and actions that determine the long-term performance of an organization. The goal of strategic security management is to ensure that an organization's security practices and policies are in line with the mission statement.

Behavioral Outcome: The individual serving as the ISSM will be knowledgeable of Departmental cybersecurity policies, strategic direction, mission objectives, infrastructure initiatives, and security funding priorities. He/she will apply this knowledge when establishing, implementing, monitoring, and communicating cybersecurity policies and strategic planning initiatives at the operating unit level.

Training concepts to be addressed at a minimum:

- Assess performance and overall effectiveness of the strategic security program with respect to Departmental directives and applicable PCSP requirements.
- Determine if security controls and processes are adequately integrated into the investment planning process based on IT portfolio and security reporting.
- Review security funding within the IT portfolio to determine if funding accurately aligns with security goals and objectives and make funding recommendations accordingly.

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 DOE/PCSP/Operating Unit policies, processes, procedures, directives, regulations, and public laws (statutes)
- Demonstrate a **functional** knowledge of methods and techniques to measure performance of SDM/operating Unit organizational cybersecurity activities in conjunction with organizational missions and business needs
- Demonstrate a **functional** knowledge of capital planning and investment control (CPIC)
- Demonstrate a **detailed** ability to analyze CPIC information involving the IT portfolio
- Demonstrate a **detailed** ability to analyze the IT portfolio for adequate security funding for each portfolio item
- Demonstrate a **detailed** ability to analyze cybersecurity costs in relation cybersecurity control requirements and the mission and goals of the SDM organization and Operating Unit mission statements

Competency Area: **System and Application Security**

Functional Requirement: **Manage**

Competency Definition: Refers to the knowledge of principles, practices, and procedures required to integrate information security into an 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: Individuals fulfilling the role of ISSM will have a working knowledge of the principles, practices, and procedures required to integrate cybersecurity into an IT system or application via the SDLC process. He/she will apply this knowledge when coordinating Software Quality Assurance policies and procedures with applicable organizations and when establishing, implementing, and monitoring the operating unit's C&A and Security Testing &Evaluation (ST&E) programs.

Training concepts to be addressed at a minimum:

- Coordinate the establishment of a formalized IT system and application security engineering program (i.e., SDLC process) in accordance with Departmental directives and applicable PCSP requirements.
- Define the scope of the cybersecurity program as it applies to application of the SDLC process.
- Acquire the necessary resources, including financial resources, to support integration of security in the SDLC.
- Ensure that cybersecurity personnel are trained in SDLC standards and processes.
- Provide feedback to developers on security issues through the SDLC process.
- Establish a C&A program for all information systems and applications.
- Collaborate with IT project management to integrate security functions into the project management process.
- Ensure that resources are available to conduct ST&E and that such testing is used to determine

the system's compliance with defined security requirements and document the effectiveness of security control implementation.
- Ensure that appropriate changes and improvement actions are implemented 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 **detailed** knowledge of DOE/PCSP/Operating Unit policies, processes, procedures, directives, regulations, and public laws (statutes)
- Demonstrate a **functional** knowledge of program management sufficient to provide a framework for project management, budget formulation, program direction, implementation strategies, plans, and procedures.
- Demonstrate a **functional** knowledge of project management principles and activities
- Demonstrate a **functional** ability to provide methods to measure the accomplishment of cybersecurity goals to assist in accomplishing DOE/PCSP policies, processes, procedures, directives, regulations, and public laws (statutes); organization mission; investment portfolio costs; and Departmental and organizational Enterprise Architecture functions
- Demonstrate a **detailed** ability to assess the effectiveness of protection measures as implemented.
- Demonstrate a **functional** knowledge of configuration management and control methodologies and available tools
- Demonstrate a **functional** ability to structure security implementations into the IT SDLC process for the Operating Unit
- Demonstrate a **functional** ability to construct ST&E schedules, activities, and costs estimates
- Demonstrate a **functional** ability to construct a framework for C&A and Continuous Monitoring activities

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 IT system or application during the 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, C&A, and software security standards compliance.

Behavioral Outcome: Individuals fulfilling the role of ISSM will have a working knowledge of the

principles, practices, and procedures required to integrate cybersecurity into an IT system or application via the SDLC process. He/she will apply this knowledge when coordinating Software Quality Assurance policies and procedures with applicable organizations and when establishing, implementing, and monitoring the operating unit's C&A and ST&E programs.

Training concepts to be addressed at a minimum:

- Integrate applicable information security requirements, controls, processes, and procedures into information system and application design specifications in accordance with Departmental directives and applicable PCSP requirements.
- Specify minimum security configurations for IT systems or applications.
- Develop processes for determining/establishing accreditation boundaries and forms of accreditation.
- Establish engineering standards to be used during the SDLC process in coordination with Software Quality Assurance organizations.
- Develop processes and procedures to mitigate the introduction of vulnerabilities during the engineering process.
- 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 **detailed** knowledge of DOE/PCSP/Operating Unit policies, processes, procedures, directives, regulations, and public laws (statutes)
- Demonstrate a **functional** knowledge of the SDLC process and available cybersecurity standards and guidelines
- Demonstrate a **functional** knowledge of methods for allocation of hardware and software to identify system components
- Demonstrate a **functional** ability to structure security implementations into the IT SDLC process for the Operating Unit
- Demonstrate a **functional** knowledge of secure system development processes and tools
- Demonstrate a **functional** knowledge of project management principles and activities

Competency Area: **System and Application Security**

Functional Requirement: **Evaluate**

Competency Definition: Refers to the knowledge of principles, practices, and procedures required to integrate information security into an IT system or application during the 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, C&A, and software security standards compliance.

Behavioral Outcome: Individuals fulfilling the role of ISSM will have a working knowledge of the principles, practices, and procedures required to integrate cybersecurity into an IT system or application via the SDLC process. He/she will apply this knowledge when coordinating Software Quality Assurance policies and procedures with applicable organizations and when establishing, implementing, and monitoring the operating unit's C&A and ST&E programs.

Training concepts to be addressed at a minimum:

- Assess and evaluate system and application security policies and procedures to ensure compliance with Departmental directives and applicable PCSP requirements.
- Review new and existing security technologies to support secure engineering across SDLC phases.
- Continually assess effectiveness of information system controls based on Departmental directives, risk management practices and procedures.
- Assess system maturation and readiness for promotion to the production stage.
- Perform continuous monitoring activities of accredited information systems and applications to identify security-significant changes that warrant re-accreditation.
- Collect lessons learned from integration of information security into the SDLC process and initiate improvement actions where 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 **detailed** knowledge of DOE/PCSP/Operating Unit policies, processes, procedures, directives, regulations, and public laws (statutes)
- Demonstrate a **detailed** ability to analyze controls for evaluating compliance of the SSP with DOE/PCSP policies, processes, procedures, directives, and regulations
- Demonstrate a **detailed** ability to analyze controls implementation for evaluating compliance with the SSP
- Demonstrate a **functional** knowledge of project management principles and activities
- Demonstrate a **functional** ability to assess control application and effectiveness
- Demonstrate a **functional** ability to evaluate assessment results and determine adequacy of

control implementation

- Demonstrate a **detailed** ability to devise adequate implementations of controls