DOE CYBERSECURITY:

CORE COMPETENCY TRAINING REQUIREMENTS

Key Cybersecurity Role: **Cybersecurity Program Manager (CSPM)**

Role Definition: The CSPM is the Senior DOE Manager of an organization or is a Federal employee appointed by the Senior DOE Manager to serve as his/her representative on all cybersecurity issues. This individual is responsible for overseeing the implementation of the cybersecurity program within the Senior DOE Manager's organization to include developing, disseminating, and maintaining the organizational Risk Management Implementation Plan (RMIP).

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 CSPM will understand the policies and procedures required to ensure the confidentiality, integrity, and availability of all categories of information. He/she will apply this knowledge when establishing, coordinating, communicating, and evaluating Senior Departmental or organizational cybersecurity policies and strategic planning initiatives.

Training concepts to be addressed at a minimum:

- Ensure that data classification and data management policies and guidance are formally issued, updated, and reviewed.

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 **functional** knowledge of data classification/sensitivity of information used within the organization
- Demonstrate the **detailed** ability to provide guidance and propose policy that incorporates data

handling appropriate to the sensitivity/classification of the information

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 CSPM will understand the policies and procedures required to ensure the confidentiality, integrity, and availability of all categories of information. He/she will apply this knowledge when establishing, coordinating, communicating, and evaluating Senior Departmental or organizational cybersecurity policies and strategic planning initiatives.

Training concepts to be addressed at a minimum:

- Assess the effectiveness of Departmental/RMIP data security policies, processes, and procedures against established standards, guidelines, and requirements and suggest changes where appropriate.

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 policies, processes, and procedures
- Demonstrate a **detailed** knowledge of established data management policies and standards within the organization
- Demonstrate a **detailed** ability to analyze and compare standards, guidelines, policies, and processes

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: The individual serving as the CSPM will understand the processes and procedures required for identifying and responding to organizational cybersecurity incidents and cybersecurity alerts; for establishing INFOCON notification and changes procedures; and for establishing investigative techniques that preserve electronic evidence and allow for data recovery and analysis. He/she will apply this knowledge when establishing, coordinating, communicating, and evaluating Senior Departmental or organizational cybersecurity policies and strategic planning initiatives.

Training concepts to be addressed at a minimum:

- Develop the incident management policy based on standards and procedures for the organization to include impact assessments and incident categorization requirements
- Develop procedures for reporting INFOCON changes and security incidents including incidents and potential incidents involving Personally Identifiable Information (PII) to DOE JC3
- Develop procedures for performing incident and INFOCON responses and maintaining records.
- Develop procedures for handling information and cyber alerts disseminated by the DOE JC3
- 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 **functional** knowledge of 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 **general** knowledge of Operating Unit incident management processes
- Demonstrate a **functional** knowledge of methods for evidence preservation and chain of custody

- Demonstrate a **functional** ability to provide policy and guidance for preservation of evidence, chain of custody, and processes to prevent loss/destruction of electronic evidence
- Demonstrate a **detailed** knowledge to interface INFOCON and incident management through organizational policy and guidance
- Demonstrate a **functional** knowledge of forensics capabilities available for use during cybersecurity incident investigation
- Demonstrate a **functional** knowledge of 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 CSPM 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 and coordinating the Senior Departmental or organizational Cybersecurity Awareness and Training (CSAT) Program.

Training concepts to be addressed at a minimum:

- Identify business requirements and establish RMIP and organizational policy for the cybersecurity awareness and training program.
- Set operational performance measures for training and delivery.
- Ensure the organization complies with cybersecurity awareness and training standards, requirements, and performance measures.

Training Evaluation Criteria: **Demonstrate**

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

Level of Demonstration:

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

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

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

- Demonstrate a **detailed** knowledge of DOE training policy, standards, and guidance
- Demonstrate a **functional** knowledge of training methodologies
- Demonstrate a **general** ability to identify cybersecurity training as it relates to organizational missions and information

- Demonstrate a **functional** knowledge of training evaluation techniques and methods
- Demonstrate a **functional** knowledge of measurement techniques and methods
- Demonstrate a **detailed** knowledge of the use of metrics for evaluations

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 CSPM 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 and coordinating the Senior Departmental or organizational Cybersecurity Awareness and Training (CSAT) Program.

Training concepts to be addressed at a minimum:

- Develop a workforce development, training, and awareness program plan in accordance with Departmental directives and applicable RMIPs.
- Ensure currency and accuracy of training and awareness materials.
- Establish a tracking and reporting strategy for the cybersecurity training and awareness 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 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: **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 CSPM 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 and coordinating the Senior Departmental or organizational Cybersecurity Awareness and Training (CSAT) Program.

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

- Assess and evaluate the cybersecurity awareness and training program for compliance with policies, regulations, and laws (statutes), and organizational performance measure objectives.
- Review cybersecurity awareness and training program materials and recommend improvements.
- Assess the awareness and training program to ensure that it meets not only the organization's stakeholder needs, but that it is effective and 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 public law, regulations, and DOE/RMIP and Operating Unit training policy, standards, and guidance
- Demonstrate a **functional** ability to analyze and compare standards , guidelines, policies, and processes
- Demonstrate a **detailed** 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: **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 CSPM will understand the policies and procedures required for an organization to comply with applicable information security laws, regulations, Departmental policy, and industry-wide best practices. He/she will apply this knowledge when establishing, coordinating, communicating, and evaluating Senior Departmental or organizational cybersecurity policies and strategic planning initiatives.

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

- Establish and administer a risk-based organizational information security program that addresses applicable Departmental standards, procedures, directives, policies, and regulations and laws (statutes).
- Define the organizational information security compliance 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 organization.
- 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 all 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.

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/RMIP and Operating Unit policy, standards, and guidance
- Demonstrate a **detailed** ability to communicate program objectives and implementation to Senior DOE Managers 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 **general** knowledge of the Privacy Act and associated regulations and policies

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 CSPM will understand the policies and procedures required for an organization to comply with applicable information security laws, regulations, Departmental policy, and industry-wide best practices. He/she will apply this knowledge when establishing, coordinating, communicating, and evaluating Senior Departmental or organizational cybersecurity policies and strategic planning initiatives.

Training concepts to be addressed at a minimum:

- Develop organizational information security compliance strategies, policies, plans, and procedures in accordance with Departmental/RMIP established standards, procedures, directives, policies, and regulations and laws (statutes).
- Specify organizational information security compliance program control requirements.
- Develop an organizational information security compliance performance 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 public law, regulations, and DOE/RMIP 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 CSPM will understand the policies and procedures required for an organization to comply with applicable information security laws, regulations, Departmental policy, and industry-wide best practices. He/she will apply this knowledge when establishing, coordinating, communicating, and evaluating Senior Departmental or organizational cybersecurity policies and strategic planning initiatives.

Training concepts to be addressed at a minimum:

- Monitor, assess, and report information security compliance practices for organizational information systems in accordance with policies and procedures.
- Maintain ongoing and effective communications with key stakeholders for compliance reporting purposes.

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/RMIP 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 analyze practices for compliance with DOE policy and procedures
- Demonstrate a **functional** knowledge of assessment reporting processes and procedures

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 CSPM will understand the policies and procedures required for an organization to comply with applicable information security laws, regulations, Departmental policy, and industry-wide best practices. He/she will apply this knowledge when establishing, coordinating, communicating, and evaluating Senior Departmental or organizational cybersecurity policies and strategic planning initiatives.

Training concepts to be addressed at a minimum:

- Assess the effectiveness of compliance program controls against Departmental/RMIP standards, policies, procedures, guidelines, directives, and regulations and laws (statutes) and implement change where appropriate.

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/RMIP 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 procedures, guidelines, directives, and regulations and laws (statutes)
- 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 **functional** knowledge of configuration control and change policies, processes, and controls

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 CSPM will be knowledgeable of Departmental risk management policies, procedures, and mitigation strategies and will apply this knowledge when establishing, coordinating, communicating, and evaluating Senior Departmental or organizational cybersecurity policies and strategic planning initiatives.

Training concepts to be addressed at a minimum:

- Establish a threat-based risk management program based on organizational missions, business goals and objectives (e.g., DOE Threat Statement, Senior DOE Management identified threats, Operating Unit identified threats, mission criticality, etc.).
- Ensure that appropriate changes and improvement actions as identified during risk analysis activities 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 **functional** knowledge of Departmental/RMIP policies and procedures for evaluating and managing risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation
- Demonstrate a **functional** knowledge of threats and threat sources
- Demonstrate a **functional** knowledge of organization missions and site/facility assignment of missions
- Demonstrate a **functional** knowledge of the DOE Risk Management Framework and the RMIP implementation
- Demonstrate a **functional** ability to analyze security risk assessments based on organizational 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 CSPM will be knowledgeable of Departmental risk management policies, procedures, and mitigation strategies and will apply this knowledge when establishing, coordinating, communicating, and evaluating Senior Departmental or organizational cybersecurity policies and strategic planning initiatives.

Training concepts to be addressed at a minimum:

- Develop and maintain risk-based security policies, plans, and procedures based on security requirements and in accordance with Departmental/RMIP standards, procedures, directives, policies, and regulations and laws (statutes).
- Develop a risk assessment process for identifying and assessing environmental (operational, logical, or physical) and system risks to information assets, personnel, facilities, and equipment and mitigating those risks.
- Develop a process for determining the security significance of proposed environmental and system changes and the resulting reaccreditation requirements.
- Develop processes and procedures for determining the costs and benefits of risk mitigation strategies.
- Develop procedures for documenting equivalency/exemption requests.

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 the DOE/RMIP policies and procedures for evaluating and managing risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation
- Demonstrate a **functional** 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/RMIP 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 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 CSPM will be knowledgeable of Departmental risk management policies, procedures, and mitigation strategies and will apply this knowledge when establishing, coordinating, communicating, and evaluating Senior Departmental or organizational cybersecurity policies and strategic planning initiatives.

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

- Assess effectiveness of the risk management program and implement changes where required.
- Assess the results of threat and vulnerability assessments to identify security risks and regularly update applicable security controls.
- 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/RMIP policies, processes, procedures, directives, regulations, and public laws (statutes)
- Demonstrate a **detailed** knowledge of the DOE/RMIP 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/RMIP risk management framework
- Demonstrate a **functional** ability to analyze DOE/RMIP description of the risk management framework

- Demonstrate a **detailed** ability to analyze vulnerabilities and threats to determine the likelihood of successful attack and resulting impacts
- Demonstrate a **detailed** knowledge of technologies used within the SDM organization 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 CSPM will be knowledgeable of Departmental cybersecurity policies, strategic direction, mission objectives, and security funding priorities and will apply this knowledge when establishing, coordinating, communicating, and evaluating Senior Departmental or organizational cybersecurity policies and strategic planning initiatives.

Training concepts to be addressed at a minimum:

- Establish organizational cybersecurity program goals that are in accordance with Departmental/RMIP standards, procedures, directives, policies, and regulations and laws (statutes).
- Establish a cybersecurity program to provide security for all systems, networks, and data that support the operations and business/mission needs of the organization.
- Integrate and align cyber security, 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 organization's mission and vision and communicate the value of cybersecurity within the organization.
- Establish overall organizational architecture goals by aligning business processes, software and hardware, local and wide area networks, people, operations, and projects with the organization's overall security strategy and the Department's Enterprise Architecture strategy.
- Balance the cybersecurity investment portfolio based on organizational and Departmental Enterprise Architecture considerations and organizational security priorities.

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, processes, procedures, directives, regulations, and public laws (statutes)
- Demonstrate a **functional** knowledge of the organization's mission and business goals and objectives
- Demonstrate a **functional** knowledge of the organizations Enterprise Architecture
- 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 cyber security
- 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/RMIP policies, processes, procedures, directives, regulations, and public laws (statutes); organization mission; investment portfolio; and Departmental and organizational 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 CSPM will be knowledgeable of Departmental cybersecurity policies, strategic direction, mission objectives, and security funding priorities and will apply this knowledge when establishing, coordinating, communicating, and evaluating Senior Departmental or organizational cybersecurity policies and strategic planning initiatives.

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 organization'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/RMIP policies, processes, procedures, directives, regulations, and public laws (statutes)
- Demonstrate a **functional** knowledge of methods and techniques to measure performance of SDM organizational cybersecurity activities in conjunction with organizational missions and business needs
- Demonstrate a **detailed** ability to integrate cybersecurity with mission and business needs to provide strategic direction for the SDM 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 CSPM will be knowledgeable of Departmental cybersecurity policies, strategic direction, mission objectives, and security funding priorities and will apply this knowledge when establishing, coordinating, communicating, and evaluating Senior Departmental or organizational cybersecurity policies and strategic planning initiatives.

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

- Provide feedback to management on the effectiveness and performance of security strategic plans in accomplishing business and mission needs/goals.
- Perform internal and external analyses to ensure the organization's cybersecurity principles and practices are in line with the organizational mission.
- 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/RMIP 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/RMIP 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

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 CSPM will be knowledgeable of Departmental cybersecurity policies, strategic direction, mission objectives, and security funding priorities and will apply this knowledge when establishing, coordinating, communicating, and evaluating Senior Departmental or organizational cybersecurity policies and strategic planning initiatives.

Training concepts to be addressed at a minimum:

- Assess performance and overall effectiveness of the strategic security program to ensure compliance with Departmental and Senior DOE Management goals, priorities, and objectives.
- Determine if security controls and processes are adequately integrated into the investment planning process based on information technology (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.
- Review cost goals of major IT investments to ensure that security costs have been identified and planned for and to ensure alignment with Departmental and Senior DOE Management mission statements.

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, 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