DOE CYBERSECURITY:

CORE COMPETENCY TRAINING REQUIREMENTS

Key Cybersecurity Role: **Authorizing Official (AO)**

Role Definition: The AO is the Senior DOE Management Federal official with the authority to formally assume responsibility and be held fully accountable for operating an information system at an acceptable level of risk.

Competency Area: **Incident Management**

Functional Requirement: **Implement**

Competency Definition: Refers to the knowledge and understanding of the processes and procedures required to prevent, detect, investigate, contain, eradicate, and recover from incidents that impact the organizational mission as directed by the DOE Joint Cybersecurity Coordination Center (JC3).

Behavioral Outcome: Individuals fulfilling the role of AO will understand the processes and accomplish procedures required to appropriately categorize and report cybersecurity incidents as dictated by DOE policy through DOE JC3 as well as coordinate and communicate incident response actions with Law Enforcement Agencies, Federal agencies, and/or external governmental entities.

Training concepts to be addressed, at a minimum:

- Assign or assist with assigning appropriate incident characterization (i.e., Type 1 or Type 2) and categorization (i.e., low, medium, high, or very high).
- Report or assist with reporting incidents within mandated timeframes as required by DOE policy through DOE JCE and other Federal agencies.
- Coordinate, interface, and work under the direction of appropriate legal authority (e.g., Inspector General, FBI) regarding cyber incident investigations that involve Federal agencies and external governmental entities (e.g., Law Enforcement, state, local, 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/Risk Management Implementation Plan (RMIP) incident response requirements and processes.

- Demonstrate a **functional** knowledge of incident types and categories.
- Demonstrate a **detailed** knowledge of reporting and documentation requirements for Incident Management and Reporting.
    - DOE JC3
    - Inspector General
    - Office of Intelligence and Counter-intelligence
    - Federal Bureau of Investigation
    - Local Law Enforcement
- Demonstrate a **functional** knowledge of Operating Unit incident management processes.
- Demonstrate a **detailed** ability to assess impact (risk) due to an incident.
- Demonstrate a **functional** knowledge of methods for evidence preservation and chain of custody.

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: Individuals fulfilling the role of AO will understand risk management policies and procedures and will be able to assess the effectiveness of the risk management program as well as understand/accept residual risk and compensatory measures as permitted by Departmental directives.

Training concepts to be addressed at a minimum:

- Assess effectiveness of the risk management program and suggest changes for improvement.
- Review the performance of, and provide recommendations for, risk management tools and techniques.
- Assess residual risk and associated mitigation techniques or procedures.
- Assess the results of threat and vulnerability assessments to identify security risks to information systems.
- Make determination on acceptance of residual risk as permitted by Departmental directives.

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Simulation**

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 risk management process.
- Demonstrate a **general** knowledge of the programs and tasks being accomplished at the Operating Unit.
- 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 and ability to identify applicability of risk management techniques.
- Demonstrate a **functional** ability to evaluate the applicability of threats and vulnerabilities to the Operating Unit Information Systems.

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: Individuals fulfilling the role of AO will coordinate all aspects of the cybersecurity program at the Operating Unit level with Senior DOE Management and other organizations.

Training concepts to be addressed at a minimum:

- Coordinate all aspects of the cybersecurity program (i.e., risk management, program management, technical security, personnel security, administrative security, policy and procedure, etc.) at the Operating Unit level with Senior DOE Management.

Training Evaluation Criteria: **Demonstrate**

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

Level of Demonstration:

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

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

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

- Demonstrate a **functional** knowledge of the Operating Unit mission and security policies.
- Demonstrate a **detailed** knowledge of DOE/RMIP security mission and policies.
- Demonstrate a **detailed** ability to analyze Operating Unit policies for compliance with its mission and DOE policies.
- Demonstrate a **functional** knowledge of the non-cybersecurity elements of the Operating Unit cybersecurity program.

- Demonstrate a **detailed** ability to communicate and coordinate program activities with organizations external to the Operating Unit.

Competency Area: **System and Application Security**

Functional Requirement: **Implement**

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

Behavioral Outcome: Individuals fulfilling the role of AO will approve the operation of an information system via accreditation or an Interim Approval to Operate (IATO) based on an acceptable level of risk.

Training concepts to be addressed at a minimum:

- Approve the operation (i.e., accreditation or re-accreditation) of an information system, grants an Interim Approval to Operate (IATO) under specific terms and conditions, or decline to accredit based on system testing and evaluation (STE) results.

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 Information System Security principles and practices.
- Demonstrate a **functional** knowledge of the System Development Life Cycle.
- Demonstrate a **functional** knowledge of Information Technology and its application to security.
- Demonstrate a **detailed** knowledge of the DOE/RMIP Risk Management Framework (RMF) and minimum security controls based on system categorization.
- Demonstrate a **detailed** ability to apply the DOE/RMIP RMF and minimum security controls to Information Systems and their modifications.