DOE CYBER SECURITY EBK: CORE COMPETENCY TRAINING REQUIREMENTS

Key Cyber Security 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: **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 Cyber Incident Response Capability (CIRC).

Behavioral Outcome: Individuals fulfilling the role of AO will have a working knowledge of policies and procedures required to identify and respond to cyber security incidents, cyber security alerts, and INFOCON changes as directed by the CIRC.

Training concepts to be addressed at a minimum:

- Establish relationships between the CIRC and internal individuals/groups (e.g., AO, classification/technical officer, Facility Security Officer, legal department, etc.) and external individuals and/or groups (e.g., CIRC, law enforcement agencies, vendors, and public relations professionals).
- Ensure that appropriate changes and improvement actions are implemented as required. *NOTE: The AO needs to monitor POA&Ms even if the AO Representative tracks the activities of a POA&M.*

Competency Area: **Incident Management**

Functional Requirement: **Implement**

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

Behavioral Outcome: Individuals fulfilling the role of AO will understand the processes and accomplish procedures required to appropriately categorize and report cyber security incidents as dictated by the DOE CIRC 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).
- Respond to and report incidents within mandated timeframes as required by DOE CIRC and other Federal agencies as appropriate.
- 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.).
- Respond proactively to changes in INFOCON levels as disseminated by Senior DOE Management or the DOE Chief Information Officer.

Competency Area: **Cyber Security 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: Individuals fulfilling the role of AO will understand the concepts of effective cyber security awareness activities to influence human behavior as well as understand the criticality of regular cyber security training for individuals with information security roles.

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

- Ensure that appropriate changes and improvement actions are implemented as required.

Competency Area: **Cyber Security 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: Individuals fulfilling the role of AO will understand the concepts of effective cyber security awareness activities to influence human behavior as well as understand the criticality of regular cyber security training for individuals with information security roles.

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

- Review cyber security awareness and training program materials and recommend improvements.

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.

Behavioral Outcome: The individual serving as the AO 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 monitoring the IT infrastructure security administration program.

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

- Ensure that appropriate changes and improvement actions are implemented as required.

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: Individuals fulfilling the role of AO will have a working knowledgeable of personnel security policies and procedures and will coordinate with the appropriate security oversight offices to ensure that personnel security access controls are implemented as required by system functional design specifications and as mandated by Departmental directives.

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

- Coordinate with physical security, operations security, and other organizational managers to ensure a coherent, coordinated, and holistic approach to security across the organization.

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 AO will have a working knowledgeable of physical security policies and procedures and will coordinate with the appropriate security oversight 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.

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

- Coordinate with personnel managing IT security, personnel security, COMSEC, operations security, and other security functional areas to provide an integrated, holistic, and coherent security effort.

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: Individuals fulfilling the role of AO will have a working knowledge of the organizational compliance program and will assess the effectiveness of assessment techniques and remedial actions and procedures.

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

- Identify major risk factors (e.g., product, compliance, and operational) and coordinate the application of information security strategies, plans, policies, and procedures to reduce regulatory risk.

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 in course curricula:

- 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 implemented by the organization.
- 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 and

the applicable Risk Management Approach.

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 cyber security program at the Operating Unit level with Senior DOE Management and other organizations.

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

- Coordinate all aspects of the cyber security 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.

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 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 in course curricula:

- Ensure that appropriate changes and improvement actions are implemented as required.

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 in course curricula:

- 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.