DOE CYBER SECURITY EBK: CORE COMPETENCY TRAINING REQUIREMENTS

Key Cyber Security Role: **Authorizing Official Designated Representative (AODR)**

Role Definition: The AODR provides technical and organizational support to the AO. The AODR functions may be performed by the AO; however, if the functions are delegated, the role should be filled by one or more technical experts responsible to the AO for ensuring that cyber security is integrated into and implemented throughout the life cycle of a system and that the Risk Management Approach (RMA) and associated policies are implemented appropriately. Individual(s) in the AO Representative role will have a working knowledge of system function, security policies, and technical security safeguards, and serve as technical advisor(s) to the AO.

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: Individuals fulfilling the role of AODR will understand and assess the policies and procedures implemented to protect all categories of information as well as have a working knowledge of technical controls used to ensure the confidentiality, integrity, and availability of data based on a formally approved need-to-know.

Training concepts to be addressed at a minimum:

- Assess the effectiveness of Departmental/RMA data security policies, processes, and procedures against established standards, guidelines, and 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.
- Assess data transmissions (e.g., email, file transfers, etc.) to evaluate the protection mechanisms being utilized (e.g., sensitivity determinations, sensitivity labels, encryption, etc.).
- Review alleged violations of data security and privacy breaches.
- 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.

Competency Area: **Enterprise Continuity**

Functional Requirement: **Evaluate**

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 AODR will have a working knowledge of the continuity of operation concepts to include disaster recovery, contingency plans, critical resource/facility continuity, delegation of authority, etc. He/she will apply this knowledge to effectively monitor the operating unit's continuity of operations program.

Training concepts to be addressed at a minimum:

- Assess the effectiveness of the continuity program, processes, and procedures and make recommendations for improvement.

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 AODR will have a working knowledge of policies and procedures required for identification, response, and reporting of cyber security incidents, cyber security alerts, and INFOCON changes as directed by the DOE CIRC.

Training concepts to be addressed at a minimum:

- Maintain current knowledge on network forensic tools 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 Cyber Incident Response Capability (CIRC).

Behavioral Outcome: Individuals fulfilling the role of AODR will have a working knowledge of policies and procedures required for identification, response, and reporting of cyber security incidents, cyber security alerts, and INFOCON changes as directed by the DOE CIRC. He/she will apply this knowledge when developing communications plans and reporting procedures.

Training concepts to be addressed at a minimum:

- Develop procedures for handling information and cyber alerts disseminated by the DOE CIRC.

Competency Area: **Incident Management**

Functional Requirement: **Evaluate**

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 AODR will have a working knowledge of policies and procedures required for identification, response, and reporting of cyber security incidents, cyber security alerts, and INFOCON changes as directed by the DOE CIRC. He/she will apply this knowledge when evaluating incident response plans and procedures at the operating unit level.

Training concepts to be addressed at a minimum:

- Identify incident management and INFOCON improvement actions based on assessments of the effectiveness of incident management and INFOCON procedures.

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 AODR 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:

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

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.

Behavioral Outcome: Individuals fulfilling the role of AODR will understand and assess the policies and procedures implemented to protect information technology infrastructure and data as well as have a working knowledge of system and/or application function.

Training concepts to be addressed at a minimum:

- Recommend appropriate forensics-sensitive policies for inclusion in the Departmental policies and operating unit security plans.

Competency Area: **IT Systems Operations and Maintenance**

Functional Requirement: **Implement**

Competency Definition: Refers to the ongoing application of principles, policies, and procedures to maintain, monitor, control, and protect IT infrastructure and the information residing on such infrastructure during the operations phase of an IT system or application.

Behavioral Outcome: Individuals fulfilling the role of AODR will understand and assess the policies and procedures implemented to protect information technology infrastructure and data as well as have a working knowledge of system and/or application function.

Training concepts to be addressed at a minimum:

- Collaborate with technical support, incident management, and security engineering teams to develop, implement, control, and manage new security administration technologies.

Competency Area: **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.

Behavioral Outcome: Individuals fulfilling the role of AODR will understand and assess the policies and procedures implemented to protect information technology infrastructure and data as well as have a working knowledge of system and/or application function. He/she will use this knowledge when performing technical reviews of planned IT infrastructure implementations and/or enhancements.

Training concepts to be addressed at a minimum:

- Assess performance, compliance, and adequacy of applied security controls in accordance with Departmental/RMA standards, procedures, directives, policies, and regulations and laws (statutes) to include configuration management, audit and analysis, vulnerability and patch management, and security performance testing.
- Assess the performance of security administration measurement technologies.
- Assess the effectiveness of the patch and vulnerability management processes.
- Assess the effectiveness of implementing corrective actions via the POA&M process and/or other internal action tracking processes.

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: Individuals fulfilling the role of AODR will understand and assess the policies and controls implemented to protect network and telecommunication services to include a working knowledge of the unique threats associated with remote access, interconnected systems, and wireless technologies.

Training concepts to be addressed at a minimum:

- Evaluate the effectiveness of implemented policies, procedures, and security controls for protecting network and telecommunication services to include identifying possible unmitigated risks to the computing infrastructure.
- Evaluate the effectiveness of policies, procedures, and controls implemented to secure interconnected systems so that such systems do not adversely affect the confidentiality, integrity, or availability of the computing infrastructure.
- 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.
- Evaluate the effectiveness of implemented policies, procedures, and minimum security controls for portable/mobile devices, External Information Systems, wireless technologies, and P2P network capabilities.

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: Individuals fulfilling the role of AODR 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:

- Assess the effectiveness of the information security compliance program controls against Departmental/RMA standards, policies, procedures, guidelines, directives, and regulations and laws (statutes).
- Assess effectiveness of the information security compliance process and procedures for process improvement and implement changes where appropriate.

Competency Area: **Security Risk Management**

Functional Requirement: **Implement**

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

Behavioral Outcome: Individuals fulfilling the role of AODR will understand the organizational risk posture and make recommendations for improvement where necessary. Further, this individual will have a working knowledge of system functional requirements and implemented controls so that he/she will be able to make informed decisions as to security significant changes.

Training concepts to be addressed at a minimum:

- Determine if proposed changes to computing infrastructure will introduce new vulnerabilities or negate the mitigation of existing risks (i.e., security significant changes) and make suggestions for reaccreditation.
- Provide input to policies, plans, procedures, and technologies to balance the level of risk associated with benefits provided by mitigating controls.
- Identify risk/functionality tradeoffs, and work with stakeholders to ensure that risk management implementation is consistent with desired organizational risk posture.

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 AODR will understand risk management policies and procedures and will be able to assess the effectiveness of the risk management program as well as make recommendations to the AO as to the acceptance of 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 and make recommendations to the AO as required.
- Assess the results of threat and vulnerability assessments to identify security risks to information systems.
- Identify changes to risk management policies and processes that will enable such policies to remain current with the emerging risk and threat environment.

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 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 AODR will understand the policies and processes required to integrate information security throughout the SDLC as well as monitor and assess currently implemented security controls and new risk management technologies.

Training concepts to be addressed at a minimum:

- Review new and existing risk management technologies and make recommendations for improvement where necessary to achieve an optimal organizational risk posture.
- Continually assess effectiveness of information system controls based on Departmental risk management practices and procedures.
- Perform continuous monitoring activities of accredited information systems and applications to identify security-significant changes that warrant reaccreditation.