DOE CYBER SECURITY EBK: CORE COMPETENCY TRAINING REQUIREMENTS

Key Cyber Security Role: **Certification Agent (CA)** **(***Also referred to as Security Control Assessor***)**

Role Definition: The CA is the individual responsible for assessing the management, operational, assurance, and technical security controls implemented on an information system via security testing and evaluation (ST&E) methods. This individual must be independent of system development, operation, and deficiency mitigation.

Competency Area: **Data Security**

Functional Requirement: **Design**

Competency Definition: Refers to the application of the principles, policies, and procedures necessary to ensure the confidentiality, integrity, availability, and privacy of data in all forms of media (i.e., electronic and hardcopy) throughout the data life cycle.

Behavioral Outcome: Individuals fulfilling the role of CA will understand the policies and procedures required to protect all categories of information as well as have a working knowledge of data access controls required to ensure the confidentiality, integrity, and availability of information. He/she will apply this knowledge when performing security testing and evaluation functions.

Training concepts to be addressed at a minimum:

- Develop security testing procedures.

Competency Area: **Data Security**

Functional Requirement: **Implement**

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 CA 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:

- Verify data security access controls, privileges, and associated profiles via the ST&E process.

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 CA 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:

- 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.).
- 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: **Implement**

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 CA will understand the procedures implemented to ensure continuity of operations and will apply this knowledge when developing and/or assisting with certification testing procedures.

Training concepts to be addressed at a minimum:

- Participate or assist with testing of contingency plans for organizational information systems.

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 CA will understand and evaluate the policies and procedures implemented to ensure continuity of operations required for essential business functions as a result of a disruption in service.

Training concepts to be addressed at a minimum:

- Assess the effectiveness of the continuity program, processes, and procedures and make recommend changes as appropriate.
- Review test, training, and exercise results to determine if information systems are available within organization or Senior DOE Management mission-requirement time frames and recommend changes as appropriate.

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 CA will have a working knowledge of policies and procedures required for identification, response, and reporting of cyber security incidents and cyber security alerts and will apply this knowledge when performing security testing and evaluation functions.

Training concepts to be addressed at a minimum:

- Assess the efficiency and effectiveness of incident response program activities to include digital forensic investigations. and make improvement recommendations as needed.
- Examine the effectiveness of penetration testing, incident response testing, INFOCON notification processes, training, and exercises.
- Examine penetration testing and vulnerability analysis results to identify risks.

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 CA 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 as needed.

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

Functional Requirement: **Evaluate**

Competency Definition: Refers to the ongoing application of principles, policies, and procedures to maintain, monitor, control, and protect IT infrastructure and the information residing on such infrastructure during the operations phase of an IT system or application. Individuals with these functions perform a variety of data collection, analysis, reporting and briefing activities associated with security operations and maintenance to ensure that the organizational security policies are implemented and maintained on information systems.

Behavioral Outcome: Individuals fulfilling the role of CA will be knowledgeable of the policies, procedures, and controls required to protect IT infrastructure and data and will be able to assess technical, operational, and/or administrative security controls as mandated by Departmental/PCSP standards.

Training concepts to be addressed at a minimum:

- Evaluate the performance and correctness of applied security controls in accordance with standards, procedures, directives, policies, and regulations and recommend corrective actions as needed.
- Assess the performance of security administration measurement technologies.
- Assess the effectiveness of the patch and vulnerability management processes.
- Identify improvement actions via a documented POA&M based on reviews, assessments, and other data sources.

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

Functional Requirement: **Evaluate**

Competency Definition: Refers to the application of 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 CA will understand the policies and procedures implemented to protect network and telecommunication services and be able to assess applicable technical security controls such as perimeter defense, defense-in-depth, and data encryption techniques.

Training concepts to be addressed at a minimum:

- Assess network, anti-malware, and perimeter defense policies in accordance with Departmental/PCSP standards, procedures, directives, policies, and regulations and recommend corrective actions if needed.

- Assess procedures and controls implemented to protect telecommunication networks from unauthorized access.
- Evaluate interconnected systems to ensure that they do not negatively impact the confidentiality, integrity, and availability of connected systems.
- Assess the implementation of remote access policies to ensure adequate protection of DOE information when processed offsite.
- 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: **Personnel Security**

Functional Requirement: **Evaluate**

Competency Definition: Refers to the knowledge of human resource selection methods and controls used by an organization to help deter willful acts of security breaches such as theft, fraud, misuse, and noncompliance. These controls include organization/functional design elements such as separation of duties, job rotation, and classification.

Behavioral Outcome: The CA will be knowledgeable of personnel access security controls such as restricted access based on appropriate security clearances and need-to-know authorizations and will apply this knowledge when performing security testing and evaluation functions.

Training concepts to be addressed at a minimum:

- Assess effectiveness of personnel security control testing.

Competency Area: **Physical and Environmental Security**

Functional Requirement: **Evaluate**

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 CA will be knowledgeable of physical access controls and environmental controls implemented to protect the organizational operating environment and will apply this knowledge when performing security testing and evaluation functions.

Training concepts to be addressed at a minimum:

- Assess effectiveness of physical and environmental security control testing.

Competency Area: **Regulatory and Standards Compliance**

Functional Requirement: **Manage**

Competency Definition: Refers to the application of 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 CA will understand the policies and procedures implemented to ensure organizational compliance with applicable laws, regulations, and/or Departmental/PCSP requirements and apply this knowledge when performing security testing and evaluation functions.

Training concepts to be addressed at a minimum:

- Identify and stay current on all external laws, regulations, standards, and best practices applicable to the organization.
- Keep informed on pending information security changes, trends, and best practices by participating in collaborative settings.
- Utilize lessons learned from organizational compliance activities to implement appropriate changes and improvement actions as required..

Competency Area: **Regulatory and Standards Compliance**

Functional Requirement: **Implement**

Competency Definition: Refers to the application of 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 CA will understand and assess policies and procedures implemented to ensure organizational compliance with applicable laws, regulations, and/or Departmental/PCSP requirements.

Training concepts to be addressed at a minimum:

- Conduct comprehensive assessments via the ST&E process to determine if information security objectives, controls, processes, and procedures are effectively applied and maintained, and perform as expected.
- Document information security audit and assessment results, recommend remedial actions and procedures, and estimated due dates for completion of remedial actions in the POA&M and in a corrective action plan as required.

Competency Area: **Regulatory and Standards Compliance**

Functional Requirement: **Evaluate**

Competency Definition: Refers to the application of 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 CA will understand and assess policies and procedures implemented to ensure organizational compliance with applicable laws, regulations, and/or Departmental/PCSP requirements.

Training concepts to be addressed at a minimum:

- Assess the effectiveness of compliance security program controls against Departmental/PCSP standards, policies, procedures, guidelines, and regulations.

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 CA will understand risk management policies and procedures and will be able to assess the effectiveness of the risk management program to include mitigation strategies.

Training concepts to be addressed at a minimum:

- Implement threat and vulnerability assessments to identify security risks and regularly update applicable security controls as required.

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 CA will understand risk management policies and procedures and will be able to assess the effectiveness of the risk management program to include mitigation strategies.

Training concepts to be addressed at a minimum:

- Assess the effectiveness of the risk management program via the ST&E process and recommend changes where required.
- Review the performance of risk management tools and techniques.
- Assess residual risk in the information infrastructure used by the organization.
- Assess the results of threat and vulnerability assessments to identify security risks and regularly update applicable security controls..

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 CA will be knowledgeable of Departmental cyber security policies, strategic direction, mission objectives, and infrastructure initiatives and will apply this knowledge when assessing risk management and mitigation during security testing and evaluation functions. .

Training concepts to be addressed at a minimum:

- Assess the integration of security policies and practices with mission requirements and recommend improvements.

Competency Area: **System and Application Security**

Functional Requirement: **Manage**

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

Behavioral Outcome: Individuals fulfilling the role of CA will understand SDLC policies and processes and will be able to assess the adequacy of implemented management, operational, assurance, and technical security controls via the ST&E process.

Training concepts to be addressed at a minimum:

- Ensure that resources are available to conduct ST&E and that such testing is used to determine the system's compliance with defined security requirements and document the effectiveness of security control implementation.

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 IT system or application during the System Development Life Cycle (SDLC). The goal of this activity is to ensure that the operation of IT systems and software does not present undue risk to the organization and information assets. Supporting activities include risk assessment, risk mitigation, security control selection, implementation and evaluation, certification and accreditation (C&A), and software security standards compliance.

Behavioral Outcome: Individuals fulfilling the role of CA will understand SDLC policies and processes and will be able to assess the adequacy of implemented management, operational, assurance, and technical security controls via the ST&E process.

Training concepts to be addressed at a minimum:

- Independently validate that engineered IT security and application security controls have been implemented correctly and are effective in their application during ST&E processes.
- Document validation results (i.e., findings and/or recommendations) via the ST&E report documentation.
- Document POA&Ms as required for security controls that have not been implemented correctly.

Competency Area: **System and Application Security**

Functional Requirement: **Evaluate**

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

Behavioral Outcome: Individuals fulfilling the role of CA will understand SDLC policies and processes and will be able to assess the adequacy of implemented management, operational, assurance, and technical security controls via the ST&E process.

Training concepts to be addressed at a minimum:

- Assess and evaluate system compliance with Departmental policies and IT system security controls documented in the System Security Plan (SSP).