DOE CYBERSECURITY:

CORE COMPETENCY TRAINING REQUIREMENTS

Key Cybersecurity 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 cybersecurity is integrated into and implemented throughout the life cycle of a system and that the Risk Management Implementation Plan (RMIP) is 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/RMIP 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.).
- 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.

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 standards and guidelines.
- Demonstrate a **functional** ability to analyze and compare standards, guidelines, policies, and processes.
- Demonstrate a **detailed** knowledge of identifying sensitive, non-SUI and SUI information.
- Demonstrate a **functional** ability to determine sensitive, non-SUI and SUI information protections.
- Demonstrate the **detailed** ability to analyze implemented controls and evaluate their effectiveness and compliance with policy, standards, and guidelines.

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.

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:

- Assess performance, compliance, and adequacy of applied security controls in accordance with Departmental/RMIP 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 implementing corrective actions via the POA&M process or other internal action tracking processes.

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 Departmental/RMIP policies, processes, procedures, directives, regulations, and public laws (statutes).
- Demonstrate a **detailed** ability to analyze the implementation of controls and propose changes in implementation when needed.
- Demonstrate a **functional** ability to analyze and identify inconsistencies of DOE/RMIP policy, standards, and regulations with public law (statutes) and national level guidelines.
- Demonstrate a **functional** knowledge and ability to utilize the POA&M process to implement improvements in controls.

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.

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 Departmental/RMIP policies, processes, procedures, directives, regulations, and public laws (statutes).
- Demonstrate a **functional** knowledge of Operating Unit implemented network and telecommunication policies, procedures, and controls and the technologies used by the Operating Unit with emphasis on remote access, wireless, P2P, and the utilization of external systems.
- Demonstrate a **functional** ability to analyze policy implementation through technical, operational, management, and assurance controls.
- Demonstrate a **functional** ability to evaluate the effectiveness of Operating Unit implemented controls.
- Demonstrate a **functional** knowledge of the vulnerabilities, issues, and threats that are related to the use of various networking technologies and the interconnection of networks/systems/ components.
- Demonstrate a **functional** ability to determine the effectiveness of network and external system user training.

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 to include procedures for process improvement against Departmental/RMIP standards, policies, procedures, guidelines, directives, and regulations and laws (statutes).

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 Departmental/RMIP policies, processes, procedures, directives, regulations, and public laws (statutes).
- Demonstrate a **functional** knowledge of Operating Unit policies, processes, and procedures that implement controls required by Departmental/RMIP policies, processes, procedures, and directives.
- Demonstrate a **functional** ability to analyze controls implementing Operating Unit policies, processes, and procedures for compliance with DOE/RMIP policies, processes, procedures, directives, and regulations.
- Demonstrate a **functional** ability to analyze controls for process improvement/continuous monitoring effectiveness in implementing compliance with DOE/RMIP policies, processes, procedures, directives, and regulations and identifying/mitigating vulnerabilities.

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.

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 **functional** knowledge of the Operating Unit computing infrastructure and technologies used.
- 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 networks/information systems.

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.

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 Operating Unit risk management framework.
- Demonstrate a **functional** ability to analyze Operating Unit implementation 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 and ability to identify applicability of risk management techniques.
- 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 Operating Unit technologies to identify new implementations of required controls.

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/RMIP risk management practices and procedures.

- Perform continuous monitoring activities of accredited information systems and applications to identify security-significant changes that warrant reaccreditation.

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 current information technology and usability within the Operating Unit networks/systems to accomplish security controls.
- Demonstrate a **functional** knowledge of continuous monitoring activities as part of the risk management framework and system development life cycle.
- Demonstrate a **detailed** ability to apply assessment techniques as part of continuous monitoring activities and determine effectiveness of implemented controls.
- Demonstrate a **functional** knowledge of the DOE/RMIP Risk Management Framework (RMF) and minimum security controls based on system categorization.
- Demonstrate a **functional** ability to apply the DOE/RMIP RMF and minimum security controls to Information Systems and their modifications.