U.S. DEPARTMENT OF ENERGY

Essential Body of Knowledge (EBK)

A Competency and Functional Framework
For
Cyber Security Workforce Development

Office of the Chief Information Officer
Office of the Associate CIO for Cyber Security

January 2013

Table of Contents

Executive Summary

The Office of the Chief Information Officer (OCIO) utilized DOE cyber security policy, industry best practices and lessons learned, and comprehensive internal needs assessments to identify fundamental cyber security functional roles and associated responsibilities. In addition, core competencies were identified that represent the 'core' skill set needed by cyber security professionals to adequately fulfill their functional roles. This collective information was further used to define the Enterprise Essential Body of Knowledge (EBK). Components of the EBK are assigned to each functional role, and customized curriculum is determined for each key role. The OCIO has determined the following roles to be key functional cyber roles within the Department: Chief Information Officer (CIO), Information Owner/Steward, Chief Information Security Officer (CISO), Authorizing Official (AO), AO Designated Representative (AODR), Common Control Provider, Information System Owner, Cyber Security Program Manager (CSPM), Information System Security Officer (ISSO), Information Security Architect, Information System Security Engineer, and the Security Control Assessor.

The DHS National Cyber Security Division (NCSD) *Information Technology (IT) Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development* was used as the foundational document for the DOE-specific EBK. Additionally, the DOE EBK incorporates other established bodies of knowledge and managerial, technical, assurance, and operational concepts and requirements from DOE Directives and OCIO reference baselines.

The EBK accomplishes two important Departmental training goals: 1) defining the baseline knowledge, skills, and abilities required for key cyber security functional roles, and 2) providing the foundational objectives for the development, selection, and presentation of training. The competencies outlined in the EBK become the basis for training "modules" that can be fit into the specific course curriculum for each of the Department-defined key roles and can be presented independently to other staff with significant impact on the security of information systems (e.g., Help Desk personnel, hardware technicians, and software developers). Training is typically delivered via online options (e.g., OLC2); however, other methods can be used such as classroom instruction and workshop/seminar.

The DOE EBK and curriculum comply with required content identified by the Office of Management and Budget (OMB) Information Systems Security Line of Business (ISSLoB), align with the National Institute of Standards and Technology (NIST) Special Publications, and address the functional roles and responsibilities discussed in Departmental directives. The modules and/or courses may be used by Senior DOE Management[1] or Operating Unit Managers as a base for supplemental organization-specific training.

[1] Senior DOE Management includes the DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, and the DOE Chief Information Officer

Finally, the DOE EBK encompasses the seven high-level cyber security categories as identified by the National Initiative for Cybersecurity Education, or NICE. NICE is a national initiative that is focused on raising cyber security awareness and developing common competencies across the nation in an effort to develop a highly-skilled cyber workforce. To this end, NICE has developed a Cybersecurity Workforce Framework that organizes cyber security functions into high-level categories, each comprising several specialty areas that can be performed by different job titles based on the organizational structure. In Appendix 2 of this document, the correlation between the core competencies identified in this EBK are correlated, or mapped to, the high-level categories as identified by NICE, therefore indicating Departmental consistency with national workforce competency initiatives.

DOE Essential Body of Knowledge (EBK)

Information and system security is by its nature multidisciplinary, and it relies on a spectrum of knowledge and performance items and skill sets associated with systems security, operational security (OPSEC), TEMPEST, physical security, personnel security and other security related areas. Cyber security professionals must have a command of their craft, both in core competencies, as well as performance items and skill sets associated with their respective functional roles.

This section contains the 13 competency areas with defining functional statements, and all work functions categorized as Manage, Design, Implement, or Evaluate. Unless otherwise noted, the following competencies apply to both unclassified and classified computing environments. Classified information technology systems are typically referred to as National Security Systems, or NSS, throughout this appendix. The 13 competencies are:

- Data Security
- Continuity of Operations
- Incident Management
- Cyber Security Training and Awareness
- IT Systems Operations and Maintenance
- Network and Telecommunications Security
- Personal Security
- Physical and Environmental Security
- Procurement
- Regulatory and Standards Compliance
- Risk Management
- Strategic Security Management
- System and Application Security

1.1 Data Security

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

1.1.1 Manage

- Ensure that data classification and data management policies and guidance are issued and updated
- Specify policy and coordinate review and approval
- Ensure compliance with data security policies and relevant legal and regulatory requirements in accordance with Departmental directives and applicable Risk Management Implementation Plans (RMIPs).
- Ensure appropriate changes and improvement actions are implemented as required
- Maintain current knowledge of authenticator management for unclassified and classified systems
- Ensure compliance with protection requirements, control procedures, incident management reporting, remote access requirements, and system management for all systems as well as use of encryption for protecting Sensitive Unclassified Information (SUI) including Personally Identifiable Information (PII) and classified information.

1.1.2 Design

- Develop data security policies using data security standards, guidelines, and requirements that include privacy, authentication, access control, retention, disposal, incident management, disaster recovery, supply chain risk management, and configuration
- Identify and document the appropriate level of protection for data, including use of encryption
- Specify data and information classification, sensitivity, and need-to-know requirements by information type on a system in terms of its confidentiality, integrity, and availability. Utilize DOE M 205.1-5 to determine the information impacts for unclassified information and DOE M 205.1-4 to determine the Consequence of Loss for classified information
- Create authentication and authorization system for users to gain access to data based on assigned privileges and permissions
- Develop acceptable use (e.g., personal use of IT policy; waste, fraud, and abuse policy, etc.) procedures in support of the data security policies
- Develop sensitive data collection and management procedures in accordance with Departmental/RMIP standards, procedures, directives, policies, and regulations, and laws (statutes)
- Identify the minimum security controls based on the system categorization. Develop or identify additional security controls based on the Consequence of Loss or Impact and the perceived risk of compromise to the data introduced by the data's logical, operational, or physical environment
- Develop security testing procedures

- Develop media sanitization (clearing, purging, or destroying) and reuse procedures
- Develop and document processes, procedures, and guidelines for complying with protection requirements (e.g., e-mail labels, media labels, etc.), control procedures (e.g., discretionary access control, need-to-know sharing, etc.), incident management reporting, remote access requirements, system management and use of encryption
- Develop procedures for the release of non-system high information to systems accredited for lower information sensitivities (classified or unclassified)
- Develop procedures for securing approval to release unclassified information to the public (DOE M 470.4-4, OPSEC).

1.1.3 Implement

- Perform the data access management process according to established guidelines
- Apply and verify data security access controls, privileges, and associated profiles
- Implement media control procedures, and continuously monitor for compliance
- Implement and verify data security access controls, and assign privileges
- Address all suspected incidents in accordance with Departmental directives and applicable RMIPs
- Apply and maintain confidentiality controls and processes in accordance with standards, procedures, directives, policies, regulations, and laws (statutes)
- Implement authenticator generation and verification requirements and processes in accordance with standards, procedures, directives, policies, regulations, and laws (statutes)
- Apply defensive countermeasures (e.g., encryption, access control, and identity management) to reduce exploitation opportunities of supply chain vulnerabilities.
- Execute media sanitization (clearing, purging, or destroying) and reuse procedures
- Execute processes and procedures for protecting SUI, including PII.

1.1.4 Evaluate

- Assess the effectiveness of Departmental/RMIP data security policies, processes, and procedures against established standards, guidelines, and requirements, and suggest changes where appropriate
- 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
- Identify improvement actions required to maintain the appropriate level of data protection

- 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.

1.2 Enterprise Continuity

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.

1.2.1 Manage

- Coordinate with stakeholders to establish the organizational continuity of operations program
- Acquire necessary resources, including financial resources, to conduct an effective continuity of operations program
- Define the continuity of operations organizational structure and staffing model
- Define emergency delegations of authority and orders of succession for key positions
- Direct contingency planning, operations, and programs to manage risk
- Define the scope of the continuity of operations program to address business continuity, business recovery, contingency planning, and disaster recovery/related activities
- Ensure that each system is covered by a contingency plan
- Integrate organizational concept of operations activities with related contingency planning activities
- Define overall contingency objectives and criteria required for activating contingency plans
- Establish a continuity of operations performance measurement program
- Identify and prioritize critical business functions to include Critical Infrastructure and Key Resources
- Provide supply chain risk guidance for development of the disaster recovery and continuity of operations plans
- Ensure that appropriate changes and improvement actions are implemented as required
- Apply lessons learned from test, training and exercise, and crisis events.

1.2.2 Design

- Develop a continuity of operations plan and related procedures in accordance with Departmental directives and applicable RMIPs
- Develop and maintain information system continuity of operations documentation such as contingency, business continuity, disaster recovery, and incident management plans and disaster recovery strategies
- Develop a process for conducting Business Impact Analyses (BIAs) to identify systems providing critical services and facilitate the creation of disaster recovery strategies

- Develop a comprehensive test, training, and exercise program to evaluate and validate the readiness of continuity of operations plans and contingency plans for information systems
- Prepare internal and external continuity of operations communications procedures and guidelines.

1.2.3 Implement

- Execute organization and information system continuity of operations and related contingency plans and procedures
- Conduct testing of contingency plans for all organizational information systems
- Provide contingency plan test reports on Critical Infrastructure and Key Resources to Senior DOE Management
- Control access to information assets during an incident in accordance with organizational policy.

1.2.4 Evaluate

- 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
- Assess the effectiveness of the continuity program, processes, and procedures, and make recommendations for improvement
- Continuously validate the organization against additional mandates, as developed, to ensure full compliance
- Collect and report performance measures and identify improvement actions.

1.3 Incident Management

Refers to knowledge and understanding of the process to prepare cyber security incident reports and 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), also referred to as the Joint Cybersecurity Coordination Center (JC3). This competency includes the knowledge of digital investigation and analysis techniques.

1.3.1 Manage

- Coordinate with stakeholders to establish the incident management program
- Establish and coordinate activities of a Cyber Security Incident Response Team (CIRT) to perform digital and network incident management activities
- Establish relationships between the CIRT and internal individuals/groups (e.g., DAA, classification/technical officer, Facility Security Officer, legal department, etc.) and external individuals/groups (e.g., JC3-CIRC, law enforcement agencies, vendors, and public relations professionals)
- Acquire and manage resources, including financial resources, for incident management functions
- Ensure users and incident management personnel are trained in incident reporting and handling procedures

- Ensure coordination between the CIRT and the security administration and technical support teams
- Provide adequate work space for the CIRT that at a minimum takes into account the electrical, thermal, acoustic, and privacy concerns (i.e., intellectual properties, classification, contraband) and security requirements (including access control and accountability) of equipment and personnel, and provide adequate report writing/administrative areas
- Apply lessons learned from information security incidents to improve incident management processes and procedures
- Ensure that appropriate changes and improvement actions are implemented as required
- Maintain current knowledge on network forensic tools and processes
- Establish an incident management measurement program.

1.3.2 Design

- Develop the incident management policy, based on standards and procedures for the organization to include impact assessments and incident categorization requirements
- Develop procedures for reporting INFOCON changes and security incidents including incidents and potential incidents involving Personally Identifiable Information (PII) to JC3-CIRC
- Identify services that the incident response team should provide
- Create an Incident Response Management Plan in accordance with DOE policies and the applicable RMIP
- Develop procedures for performing incident and INFOCON responses and maintaining records
- Develop procedures for handing information and cyber alerts disseminated by the JC3-CIRC
- Create incident response exercises and penetration testing activities
- Specify incident response staffing and training requirements to include general users, system administrators, and other affected personnel
- Establish an incident management measurement program
- Develop policies for preservation of electronic evidence, data recovery and analysis, and the reporting and archival requirements of examined material in accordance with procedures set forth by the JC3-CIRC
- Adopt or create chain of custody procedures that include disposal procedures and, when required, the return of media to its original owner in accordance with procedures set forth by the JC3-CIRC.

1.3.3 Implement

- Apply response actions in reaction to security incidents, in accordance with established policies, plans, and procedures to include appropriate incident characterization (i.e., Type 1 or Type 2) and categorization (i.e., low, media, high, or very high)

- Respond to and report incidents within mandated timeframes as required by the JC3-CIRC and other federal agencies (e.g., Office of Health, Safety, and Security) as appropriate
- Perform assessments to determine the impact of the loss of confidentiality, integrity, and/or availability
- Respond proactively to information and alerts disseminated by the JC3-CIRC to include performing consequence analyses and corrective actions
- Respond proactively to changes in INFOCON levels as disseminated by Senior DOE Management/DOE CIO
- Assist in collecting, processing, and preserving evidence according to Departmental/RMIP standards, procedures, directives, policies, and regulations and laws (statutes)
- Perform forensic analysis on networks and computer systems, and make recommendations for remediation
- Apply and maintain intrusion detection systems; intrusion prevention systems; network mapping software; and monitoring and logging systems; and analyze results to protect, detect, and correct information security-related vulnerabilities and events
- Follow proper chain-of-custody best practices in accordance with procedures set forth by the JC3-CIRC
- Collect and retain audit data to support technical analysis relating to misuse, penetration, reconstruction, or other investigations
- Provide audit data to appropriate law enforcement or other investigating agencies, to include Departmental security elements
- Report complete and accurate findings, and result of the analysis of digital evidence, to appropriate resources
- Execute incident response plans
- Execute penetration testing activities and incidence response exercises
- Ensure lessons learned from incidents are collected in a timely manner, and are incorporated into plan reviews
- Collect, analyze, and report incident management measures
- Coordinate, integrate, and lead team responses with internal and external groups according to applicable policies and procedures
- Coordinate, interface, and work under the direction of appropriate legal authority (e.g., Inspector General, FBI) regarding investigations or other legal requirements including investigations that involve external governmental entities (e.g., international, national, state, local).

1.3.4 Evaluate

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

- Assess the effectiveness of communications between the CIRT and related internal and external organizations, and implement changes where appropriate
- Identify incident management and INFOCON improvement actions based on assessments of the effectiveness of incident management and INFOCON procedures.

1.4 Cyber Security Training and Awareness

Refers to the 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. Training activities are designed to instruct workers about their security responsibilities and teach them about information security processes and procedures to enable duties to be performed optimally and securely within related environments. Awareness activities present essential information security concepts to the workforce to influence user behavior.

1.4.1 Manage

- Identify business requirements and establish RMIP and organizational policy for the cyber security awareness and training program
- Acquire and manage necessary resources, including financial resources, to support the cyber security awareness and training program
- Set operational performance measures for training and delivery, and ensure that they are met
- Ensure the organization complies with cyber security awareness and training standards and requirements
- Ensure that appropriate changes and improvement actions are implemented as required.

1.4.2 Design

- Develop the policy for the cyber security training and awareness program
- Incorporate requirements from the department cyber security training and awareness program
- Define the goals and objectives of the cyber security awareness and training program
- Work with appropriate security SMEs to ensure completeness and accuracy of the security training and awareness program
- Establish a tracking and reporting strategy for cyber security training and awareness program
- Ensure currency and accuracy of training and awareness materials
- Develop a workforce development, training, and awareness program plan in accordance with Departmental directives and applicable RMIPs.

1.4.3 Implement

- Perform a needs assessment to determine skill gaps and identify personnel in roles requiring training based on mission requirements in accordance with Departmental directives and applicable RMIPs

- Develop new—or identify existing—awareness and training materials that are appropriate and timely for intended audiences
- Deliver awareness and training to intended audiences based on identified needs and within DOE mandated time frames
- Update awareness and training materials when necessary
- Communicate management's commitment, and the importance of the cyber security awareness and training program, to the workforce.

1.4.4 Evaluate

- Assess and evaluate the cyber security awareness and training program for compliance with policies, regulations, and laws (statutes), and measure program and employee performance against objectives
- Review cyber security awareness and training program materials and recommend improvements
- Assess the awareness and training program to ensure that it meets not only the organization's stakeholder needs, but that it is effective and covers current cyber security issues and legal requirements
- Ensure that information security personnel are receiving the appropriate level and type of training
- Collect, analyze, and report performance measures.

1.5 IT Systems Operations and Maintenance

Refers to the ongoing application of principles, policies, and procedures to maintain, monitor, control, and protect information technology (IT) infrastructure and the information residing on it during the operations phase of an IT system or application in production. 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.

1.5.1 Manage

- Establish security administration program goals and objectives
- Monitor the security administration program budget
- Direct security administration personnel
- Address security administration program risks
- Define the scope of the security administration program
- Establish communications between the security administration team and other security-related personnel (e.g., technical support, incident management)
- Integrate security administration team activities with other security-related team activities (e.g., technical support, incident management, security engineering)
- Acquire necessary resources, including financial resources, to execute the security administration program
- Ensure operational compliance with applicable standards, procedures, directives, policies, regulations, and laws (statutes)
- Ensure that IT systems operations and maintenance enables day-to-day business functions

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

1.5.2 Design

- Develop security administration processes and procedures in accordance with Departmental/RMIP standards, procedures, directives, policies, and regulations and laws (statutes)
- Develop personnel, application, middleware, operating system, hardware, network, facility, and egress security controls
- Develop a vulnerability and patch management process
- Develop security monitoring, test scripts, test criteria, and testing procedures
- Develop security administration change management procedures to ensure that security policies and controls remain effective following a change to include identification of roles and responsibilities for change approval/disapproval
- Recommend appropriate forensics-sensitive policies for inclusion in the RMIP and Operating Unit security plans
- Define information technology security performance measures
- Develop a continuous monitoring, audit, and analysis process that includes configuration management; security control monitoring through reviews and assessments of the system and its operational, logical, and physical environment; a vulnerability scanning program; and status reporting and documentation maintenance
- Develop role-based access, based on the concept of least privilege
- Maintain the daily/weekly/monthly process of backing up IT systems to be stored both on- and off-site in the event that a restoration should become necessary
- Develop a plan to measure the effectiveness of security controls, processes, policies and procedures.

1.5.3 Implement

- Perform security administration processes and procedures in accordance with Departmental/RMIP standards, procedures, directives, policies, and regulations and laws (statutes)
- Establish a secure computing environment by monitoring, controlling, and managing unauthorized changes in system configuration, software, and hardware
- Perform monitoring and analysis of system audit records for indications of inappropriate or unusual activity
- Ensure that information systems are assessed regularly for vulnerabilities, and that appropriate solutions to eliminate or otherwise mitigate identified vulnerabilities are implemented
- Perform patch management processes that provide for the timely and prioritized remediation of identified system flaws
- Perform security performance testing and reporting, and recommend security solutions in accordance with Departmental/RMIP standards, procedures, directives, policies, and regulations and laws (statutes)
- Perform security administration changes and validation testing

- Uniquely identify (i.e., label), control, and track all IT configuration items through the continuous monitoring process
- Uniquely identify configuration changes and maintain a history of the change control methodology and tools used for information systems with security categories of Moderate and High and for all National Security Systems (NSS)
- Collaborate with technical support, incident management, and security engineering teams to develop, implement, control, and manage new security administration technologies
- Monitor vendor agreements and Service Level Agreements (SLA) to ensure that contract and performance measures are achieved
- Establish and maintain system controls and surveillance routines to monitor and control conformance to all Departmental/RMIP information security regulations and laws (statutes)
- Perform proactive security testing
- Create a Plan of Actions and Milestones (POA&M) for correction of vulnerabilities and compensation for risks or threats.

1.5.4 Evaluate

- Review strategic security technologies
- Review performance and correctness of applied security controls in accordance with Departmental/RMIP standards, procedures, directives, policies, and regulations and laws (statutes), and apply corrections as required
- Assess the performance of security administration measurement technologies
- Assess the effectiveness of the patch and vulnerability management processes
- Assess compliance with Departmental/RMIP standards, procedures, directives, policies, and regulations and laws (statutes)
- Identify improvement actions through a POA&M based on reviews, assessments, and other data sources
- Collect cyber security performance measures to ensure optimal system performance.

1.6 Network and Telecommunications Security and Remote Access

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 it resides. Examples of these practices include perimeter defense strategies, defense-in-depth strategies, and data encryption techniques. It is understood that certain telecommunication and network policies are mandated by non-cyber organizations within the DOE environment. However, cyber security professionals must be knowledgeable of telecommunication requirements and will typically collaborate with responsible organizations such as local information technology departments or Communications Security (COMSEC) personnel when developing policy in an effort to address all cyber requirements.

1.6.1 Manage

- Collaborate with responsible organizations to establish a network and telecommunications security program in line with Departmental goals and policies
- Establish communications between the network and telecommunications security team and related security teams (e.g., technical support, cyber security administration, incident response, etc.)
- Ensure the development of a risk-based approach for implementing system interconnections and wireless technologies
- Ensure compliance with applicable network-based and remote access Departmental/RMIP standards, procedures, directives, policies, and regulations and laws (statutes)
- Ensure that network-based and remote access audits and management reviews are conducted to implement process improvement
- Ensure policies and processes governing the conditions under which remote access can be granted and terminated
- Establish specific training and support requirements for External Information Systems and portable/mobile devices including protection of government information, secure operation, implementation of minimum security controls, individual rules of behavior, and consequences for rule violation
- Ensure the use and management of Peer-to-Peer (P2P) networking is defined and documented in accordance with Departmental directives and applicable RMIPs

1.6.2 Design

- Develop network and host-based security policies in accordance with Departmental/RMIP standards, procedures, directives, policies, and regulations and laws (statutes)
- Specify strategic security plans for network telecommunications in accordance with Departmental/RMIP policy and defense-in-depth strategies to meet organizational security goals
- Develop processes and procedures for protecting telecommunications networks against unauthorized access and wiretapping (e.g., protected distribution systems, transmission encryption, locked telephone closets, etc.)
- Develop processes and procedures for mitigating the loss of confidentiality of SUI or classified information by utilizing TEMPEST, emanations and Technical Surveillance Countermeasures (TSCM)
- Develop process for interconnecting information systems based on identifying organizational needs, associated risks, and controlled interface requirements
- Develop effective network domain security controls in accordance with organizational , network and host-based policies
- Develop network security performance reports
- Develop network security and telecommunication audit processes, guidelines, and procedures
- Develop wireless technology processes, guidelines, and procedures in accordance with Departmental directives and applicable RMIPs

- Develop and document processes, procedures, and guidelines related to P2P networking commensurate with the level of security required for the organization's environment and specific needs *and* in accordance with Departmental directives and applicable RMIPs
- Develop processes, procedures, and identify minimum security controls for External Information Systems and portable/mobile devices. This encompasses security controls for these systems and devices operating in a standalone operation and operating within the proximity of or connected to systems accredited for storing/ processing SUI or classified information.

1.6.3 Implement

- Prevent and detect intrusions, and protect against malware
- Perform audit tracking and reporting
- Apply and manage effective network domain security controls in accordance with organizational, network, and host-based policies
- Test strategic network security technologies for effectiveness
- Monitor and assess network security vulnerabilities and threats using various technical and non-technical data
- Mitigate network security vulnerabilities as prioritized by the organization in response to problems identified in vulnerability reports
- Provide real-time network intrusion response
- Ensure that messages are confidential and free from tampering and repudiation
- Defend network communications from tampering and/or eavesdropping
- Document interconnected system specifics (e.g., purpose, risk, information types, technical implementation, etc.) in accordance with Departmental directives and applicable RMIPs
- Compile data into measures for analysis and reporting
- Implement policies, procedures, and minimum security controls for the use of External Information Systems, wireless information technology, and portable/mobile devices in accordance with Departmental directives and applicable RMIPs
- Implement policies and procedures related to P2P networking in accordance with Departmental directives and applicable RMIPs.

1.6.4 Evaluate

- Perform a network security evaluation, calculate risks to the organization, and recommend remediation activities
- Ensure that interconnected systems do not adversely affect the confidentiality, integrity, or availability of the connected systems
- 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
- Assess fulfillment of functional requirements by arranging independent verification and validation of the network

- Analyze data and report results
- Ensure that anti-malware systems are operating correctly
- Compile data into measures for analysis and reporting
- Evaluate the effectiveness of implemented policies, procedures, and minimum security controls for portable/mobile devices, External Information Systems, wireless technologies, and P2P network capabilities.

1.7 Personnel Security

Refers to methods and controls used to ensure that an organization's selection and application of human resources (both employee and contractor) are controlled to promote security. Personnel security controls are used to prevent and detect employee-caused security breaches such as theft, fraud, misuse of information, and noncompliance. These controls include organization/functional design elements such as separation of duties, job rotation, and classification.

1.7.1 Manage

- Coordinate with physical security, operations security, and other organizational managers to ensure a coherent, coordinated, and holistic approach to security across the organization
- Ensure personnel security compliance with Departmental/RMIP standards, procedures, directives, policies, and regulations and laws (statutes)
- Ensure compliance through periodic audits of methods and controls.
- Recommend the implementation of appropriate changes and improvement actions as required

1.7.2 Design

- Establish personnel security processes and procedures for individual job roles
- Establish procedures for coordinating with other organizations to ensure that common processes are aligned
- Establish personnel security rules and procedures to which external suppliers (e.g., vendors, contractors) must conform.

1.7.3 Implement

- Coordinate within the personnel security office, or with Human Resources, to ensure that position sensitivity is established prior to the interview process, and that appropriate background screening and suitability requirements are identified for each position
- Coordinate within the personnel security office, or with Human Resources, to ensure background investigations are processed based on level of trust and position sensitivity
- Coordinate with physical security and IT security operations personnel to ensure that employee access to physical facilities, media, and IT systems/networks is modified or terminated upon reassignment, change of duties, resignation, or termination.

1.7.4 Evaluate

- Review effectiveness of the overall personnel security program in coordination with the responsible organization and recommend changes that will improve internal practices and/or security organization-wide
- Assess the relationships between personnel security procedures and organization-wide security needs, and make recommendations for improvement
- Review incident data and make process improvement recommendations
- Assess effectiveness of personnel security control testing.

1.8 Physical and Environmental Security

Physical and environmental security protects an organization's personnel, electronic equipment, and data/information based on the security objectives of confidentiality, integrity, and availability. It also refers to methods and controls used to proactively protect an organization from natural or man-made threats to physical facilities and buildings, as well as to the physical locations where IT equipment is located or work is performed (e.g., computer rooms, work locations).

1.8.1 Manage

- 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
- Recommend the implementation of appropriate changes and improvement actions as required.

1.8.2 Design

- Identify the physical security program requirements and specifications in relationship to system security goals
- Develop policies and procedures for identifying and mitigating physical and environmental threats (to include TEMPEST concerns) to information assets, personnel, facilities, and equipment
- Develop a physical security and environmental security plan, including security test plans and contingency plans, in coordination with other security planning functions
- Develop countermeasures against identified risks and vulnerabilities
- Recommend criteria for inclusion in the acquisition of facilities, equipment, and services that impact physical security.

1.8.3 Implement

- Apply physical and environmental controls in support of physical and environmental security plans
- Control access to information assets in accordance with Departmental/RMIP standards, procedures, directives, policies, and regulations and laws (statutes)
- Integrate physical security concepts into test plans, procedures, and exercises
- Conduct threat and vulnerability assessments to identify physical and environmental risks and vulnerabilities, and update applicable controls as necessary

- Compile, analyze, and report performance measures.

1.8.4 Evaluate

- Assess and evaluate the overall effectiveness of physical and environmental security policy and controls in coordination with the responsible organization and make recommendations for improvement
- Review incident data and make process improvement recommendations
- Assess effectiveness of physical and environmental security control testing
- Evaluate acquisitions that have physical security implications and report findings to management
- Assess the accuracy and effectiveness of the physical security performance measurement system, and make recommendations for improvement where applicable.

1.9 Procurement

Refers to the application of principles, policies, and procedures required to plan, apply, and evaluate the purchase of IT products or services—including "risk-based" pre-solicitation, solicitation, source selection, award, and monitoring, disposal, and other post-award activities. Procurement activities may consist of the development of procurement and contract administration documents that include, but are not limited to, procurement plans, estimates, requests for information, requests for quotes, requests for proposals, statements of work, contracts, cost-benefit analyses, evaluation factors for award, source selection plans, incentive plans, service level agreements (SLA), justifications required by policies or procedures, and contract administration plans.

1.9.1 Manage

- Collaborate with various stakeholders (including internal clients and purchasing organizations , lawyers, Chief Information Officers, Chief Information Security Officers, cyber security professionals, privacy professionals, security engineers, suppliers, etc.) on the procurement of IT security products and services
- Ensure the inclusion of risk-based cyber security requirements in acquisition plans, cost estimates, statements of work, contracts, and evaluation factors for award, service level agreements, and other pertinent procurement documents
- Ensure that investments are aligned with organizational architecture and security requirements
- Conduct detailed IT investment reviews and security analyses, and review IT investment business cases for security requirements and document in a POA&M
- Specify policies for use of government information by vendors/partners and connection requirements/acceptable use policies for vendors that connect to government networks

1.9.2 Design

- Develop contracting language that mandates the incorporation of cyber security requirements in all information technology products and/or services being purchased
- Develop contract administration policies that direct the evaluation and acceptance of delivered cyber security products and services under a contract, as well as the security evaluation of hardware and software being procured
- Develop measures and reporting standards to measure and report on key objectives in procurements aligned with cyber security policies and procedures
- Develop a vendor management policy addressing the use of government information and connection requirements and acceptable use policies for vendors who connect to Departmental networks.

1.9.3 Implement

- Include cyber security considerations as directed by Departmental/RMIP policies and procedures in procurement and acquisition activities to include the use of Evaluated and Validated Products as published by National Institute of Standards and Technology (NIST) or the National Security Agency
- Assist with negotiating final procurements (e.g., contracts, contract changes, grants, agreements, etc.) to include cyber security requirements that minimize risk to the organization
- Implement a risk-based defense-in-depth supply chain risk strategy as required by organizational policies and procedures.
- Perform compliance reviews of delivered products and services to assess the delivery of cyber requirements against stated contract requirements and measures
- Apply vendor management policies to ensure the appropriate use and protection of government information to include due diligence activities to validate that vendors are operationally and technically competent to comment and communicate with Departmental networks.

1.9.4 Evaluate

- Review contracting documents, such as statements of work or requests for proposals, for inclusion of cyber security considerations in accordance with information security requirements, policies, and procedures
- Review Memoranda of Agreement, Memoranda of Understanding, and/or SLA for agreed levels of cyber security responsibility
- Assess and evaluate the effectiveness of the vendor management program in complying with internal policy with regard to use of government information and connection
- Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities, and recommend improvements.

1.10 Regulatory and Standards Compliance

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.

1.10.1 Manage

- Establish and administer a risk-based organizational information security program that addresses applicable Departmental standards, procedures, directives, policies, and regulations and laws (statutes)
- Define the organizational information security compliance program to include the development, management, and reporting of POA&Ms
- Coordinate and provide liaison with staffs that are responsible for information security compliance, licensing and registration, and data security surveillance
- Collaborate with organizations responsible for the development and implementation of Privacy Impact Assessments
- Identify and stay current on all external laws, regulations, standards, and best practices applicable to the organization
- Identify major risk factors (product, compliance, and operational) and coordinate the application of information security strategies, plans, policies, and procedures to reduce regulatory risk
- Maintain relationships with all regulatory information security organizations and appropriate industry groups, forums, and stakeholders
- Keep informed on pending information security changes, trends, and best practices by participating in collaborative settings
- Acquire the necessary resources to support an effective information security compliance program
- Utilize lessons learned from organizational compliance activities to implement appropriate changes and improvement actions as required.

1.10.2 Design

- Develop organizational information security compliance strategies, policies, plans, and procedures in accordance with Departmental/RMIP established standards, procedures, directives, policies, and regulations and laws (statutes)
- Specify organizational information security compliance program control requirements
- Develop a POA&M and associated mitigation strategies to address program and system-level deficiencies
- Develop an organizational information security compliance performance measures program

1.10.3 Implement

- Monitor, assess, and report information security compliance practices for organizational information systems in accordance with policies and procedures
- Maintain ongoing and effective communications with key stakeholders for compliance reporting purposes
- Conduct internal audits to determine if information security control 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.

1.10.4 Evaluate

- Assess the effectiveness of compliance program controls against Departmental/RMIP 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
- Compile, analyze, and report performance measures.

1.11 Security Risk Management

Security risk management refers to the policies, processes, procedures, and technologies used by an organization 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.

1.11.1 Manage

- Establish a threat-based risk management program based on organizational missions, business goals and objectives (e.g., DOE Threat Statement, Senior DOE Management identified threats, Operating Unit identified threats, mission criticality, Supply Chain Risk Management strategy, etc.)
- Ensure the impact of security risks on mission, business goals, objectives, plans, programs, and actions are presented to DAA/ Senior DOE Management during the accreditation decision making process
- Ensure policies and procedures are in place to assess the criticality of information and communication (ICT) systems
- Acquire and manage the resources, including financial resources, necessary to conduct an effective risk management program
- Ensure that appropriate changes and improvement actions as identified during risk analysis activities are implemented as required
- Ensure that the equivalency/exemption process is in place and functional.

1.11.2 Design

- Develop and maintain risk-based security policies, plans, and procedures based on security requirements and in accordance with Departmental/RMIP standards, procedures, directives, policies, and regulations and laws (statutes)
- Develop a Security Test and Evaluation (ST&E) process for evaluating the functionality and effectiveness of each system's security controls
- Develop a risk assessment process for identifying and assessing environmental (operational, logical, or physical) and system risks to information assets, personnel, facilities, and equipment and mitigating those risks
- Develop a process for determining the security significance of proposed environmental and system changes and the resulting reaccreditation requirements

- Develop processes and procedures for determining the costs and benefits of risk mitigation strategies
- Develop procedures for documenting the decision to apply mitigation strategies or acceptance of risk
- Develop procedures for documenting equivalency/exemption requests.

1.11.3 Implement

- Apply controls for each information system by determining the system category (e.g., high, medium, low, or Protection Index) as directed by Departmental directives
- Establish accreditation boundaries based on the system category, information confidentiality, and the form of accreditation (system, type or site accreditation)
- Determine if proposed changes will introduce new vulnerabilities or negate the mitigation of existing risks (i.e., security significant changes) and reaccredit as required
- Provide input to policies, plans, procedures, and technologies to balance the level of risk associated with benefits provided by mitigating controls
- Implement threat and vulnerability assessments to identify security risks, and regularly update applicable security controls
- Implement information and communication technology (ICT) supply chain risk management policies, requirements, and procedures
- Identify risk/functionality tradeoffs, and work with stakeholders to ensure that risk management implementation is consistent with desired organizational risk posture.

1.11.4 Evaluate

- Assess effectiveness of the risk management program, and implement changes where required
- Review the performance of, and provide recommendations for, risk management (e.g., security controls, policies/procedures that make up risk management program) 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
- Make determination on acceptance of residual risk as permitted by Departmental directives and the applicable RMIP
- Identify changes to risk management policies and processes that will enable them to remain current with the emerging risk and threat environment.

1.12 Strategic Security Management

Refers to the principles, practices, and methods involved in making managerial decisions and actions that determine the long-term performance of an organization. Strategic security management requires the practice of external business analyses such as customer analyses and industry environmental analyses. It also requires the performance of internal business analyses that address financial performance, performance measurement, quality assurance, risk management, and organizational capabilities/constraints. The goal of

these analyses is to ensure that an organization's security principles, practices, and system design are in line with its mission statement.

1.12.1 Manage

- Establish a cyber security program to provide security for all systems, networks, and data that support the operations and business/mission needs of the organization
- Integrate and align cyber security, physical security, personnel security, and other security components into a systematic process to ensure that information protection goals and objectives are reached
- Establish information and communication technology (ICT) supply chain risk management (SCRM) policies and procedures.
- Align cyber security priorities with the organization's mission and vision, and communicate the value of cyber security within the organization
- Coordinate all aspects of the cyber security program at the Operating Unit level with Senior DOE Management
- Acquire and manage the necessary resources, including financial resources, to support cyber security goals and objectives and reduce overall organizational risk
- Establish overall organizational architecture goals by aligning business processes, software and hardware, local and wide area networks, people, operations, and projects with the organization's overall security strategy and the Department's Enterprise Architecture strategy
- Acquire and manage the necessary resources, including financial resources, for instituting security policy elements in the operational environment
- Establish organizational goals that are in accordance with Departmental/RMIP standards, procedures, directives, policies, and regulations and laws (statutes)
- Balance the cyber security investment portfolio based on organizational and Departmental Enterprise Architecture considerations and organizational security priorities.

1.12.2 Design

- Establish a performance management program that will measure the efficiency, effectiveness, and maturity of the cyber security program in support of the organization's business/mission needs
- Develop information security management strategic plans
- Integrate applicable laws and regulations into information security strategy, plans, policies, and procedures.

1.12.3 Implement

- Provide feedback to management on the effectiveness and performance of security strategic plans in accomplishing business/mission needs
- Perform internal and external analyses to ensure the organization's cyber security principles and practices are in line with the organizational mission
- Integrate business goals with information security program policies, plans, processes, and procedures
- Collect, analyze, and report performance measures

- Use performance measures to inform strategic decision making.

1.12.4 Evaluate

- Determine if security controls and processes are adequately integrated into the investment planning process based on IT portfolio and security reporting
- Review security funding within the IT portfolio to determine if funding accurately aligns with security goals and objectives, and make funding recommendations accordingly
- Assess the integration of security with business/mission, and recommend improvements
- Review cost goals of each major investment
- Assess performance and overall effectiveness of the strategic security program with respect to security goals and objectives
- Assess and refresh the performance measurement program to ensure currency with Departmental and Senior DOE Management goals and priorities.

1.13 System and Application Security

Refers to the principles, policies, and procedures pertaining to integrating information security into an IT system or application during the System Development Life Cycle (SDLC) prior to the Operations and Maintenance phase. This approach ensures that the operation of IT systems and software does not present undue risk to the organization and its information assets. Supporting activities include risk assessment; risk mitigation; security control selection; implementation and evaluation; certification and accreditation; and software security standards compliance.

1.13.1 Manage

- Establish the IT system and application security engineering program
- Acquire the necessary resources, including financial resources, to support integration of security in the SDLC
- Guide cyber security personnel through the SDLC phases
- Provide feedback to developers on security issues through the SDLC
- Define the scope of the cyber security program as it applies to application of the SDLC
- Establish a Certification and Accreditation (C&A) program for all information systems and applications
- Collaborate with IT project management to integrate security functions into the project management process
- Ensure that resources are available to conduct Security Testing and Evaluation (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
- Ensure that appropriate changes and improvement actions are implemented as required.

1.13.2 Design

- Specify the organizational and IT system and application security policies, standards, and best practices
- Identify accreditation boundaries and form of accreditation
- Integrate applicable information security requirements, controls, processes, and procedures into information system and application design specifications in accordance with Departmental/RMIP established standards, policies, procedures, guidelines, directives, and regulations and laws (statues)
- Specify minimum security configurations for the IT system or application as required by Departmental directives and applicable RMIPs
- Identify standards against which to engineer the IT system or application
- Develop processes and procedures to mitigate the introduction of vulnerabilities during the engineering process
- Specify the requirements and responsibilities for developing information system or application accreditation packages (i.e., security plan, security test and evaluation, etc.) in accordance with Departmental directives and applicable RMIP

1.13.3 Implement

- Execute the Departmental/RMIP information system and application security policies
- Apply and verify compliance with identified standards against which to engineer the IT system or application
- Perform processes and procedures to mitigate the introduction of vulnerabilities during the engineering process
- Implement information and communication technology (ICT) supply chain risk management policies, requirements, and procedures
- Execute the C&A process to include determining the system categorization, identifying the minimum security controls and any additional security controls needed, implementing the security controls, and authoring the IT system or application System Security Plan (SSP)
- Execute configuration management practices as required by Departmental/RMIP policies and processes, the SSP, Configuration Management Plan (CMP), Contingency Plans, etc.
- Independently validate that engineered IT security and application security controls have been implemented correctly and are effective in their application during ST&E
- Document POA&Ms as required for security controls that have not been implemented correctly
- Document validation results (i.e., findings and/or recommendations)
- Reengineer security controls to mitigate vulnerabilities identified during the certification phase
- Obtain information system or application accreditation or Interim Authorization to Operate (IATO) prior to going operational (i.e., processing live data)
- Approve the operation (accreditation or re-accreditation) of an information system, grant an IATO under specific terms and conditions, or decline to accredit.

- Ensure the integration of information security practices throughout the SDLC process
- Practice secure coding practices
- Implement and test backup-and-restore procedures for critical systems

1.13.4 Evaluate

- Review new and existing risk management technologies to achieve an optimal organizational risk posture
- Review new and existing security technologies to support secure engineering across SDLC phases
- Continually assess effectiveness of the information system's controls based on Departmental/RMIP risk management practices and procedures
- Assess and evaluate system compliance with Departmental and Senior DOE Management policies and Enterprise Architectures
- Assess system maturation and readiness for promotion to the production stage
- Perform continuous monitoring activities of accredited information systems and applications to identify security-significant changes that warrant re-accreditation
- Collect lessons learned from integration of information security into the SDLC, and use to identify improvement actions
- Collect, analyze, and report performance measures

Appendix 1: Cyber Security Role-Based EBK: Key Terms and Concepts

The purpose of this appendix is to provide a basic understanding of key terms and concepts associated with each specific competency. . Knowledge of these terms and concepts is the foundation for effective performance of functions associated with each of the technical competency areas.
At minimum, individuals should know, understand, and be able to apply those that relate to the competencies to which their role is linked. . .

2.1 Data Security	
Refers to the application of principles, policies, and procedures necessary to ensure the confidentiality, integrity, availability, and privacy of data in all forms of media (electronic and hardcopy) throughout the data life cycle.	
Acceptable/Limited Use	Need-to-Know
Access Control	Nonrepudiation
Aggregation	Personally Identifiable Information
Antivirus Software	Privacy
Authentication	Privilege Levels
Authorization	Protection Index
Categorize information & system	Public Key Infrastructure
Consequence of Loss	Role-Based Access Control
Data Classification	Rule-Based Access Control
Decryption	Sanitization
Digital Signatures	Secure Data Handling
Discretionary Access Control	Security Clearance
Electronic Commerce	Sensitive Unclassified Information
Encryption	Sensitivity Determination
Firewall Configuration	Sensitivity of Data
Identity Data and Access Management	Steganography
Identity Management	Supply Chain Vulnerability
Information Classification Scheme	System High
Least Privilege	System of Record
Mandatory Access Control	User Privileges
	User Provisioning

2.2 Enterprise Continuity	
Refers to the application of principles, policies, and procedures used to ensure that an organization continues to perform essential business functions after the occurrence of a wide range of potential catastrophic events.	
Alternate Facility	Information Technology Contingency Plan
Backup Strategy	Interoperable Communications
Business Continuity Plan	Key Resources
Business Impact Analysis	Mission Assurance
Business Recovery Plan	Occupant Emergency Plan
Contingency Plan	Order of Succession
Crisis Communication	Preparedness/Readiness
Critical Infrastructure	Risk Mitigation
Cyber Incident Response	Standard Operating Procedures
Delegation of Authority	Supply Chain Risk
Disaster Recovery	Test, Training, and Exercise
Disruption	Threat Environment
Essential Functions	Vital Records and Databases

2.3 Incident Management	
Refers to knowledge and understanding of the process to prepare and prevent, detect, contain, eradicate, recover, and apply lessons learned from incidents impacting the mission of an organization. Also refers to the knowledge and understanding of digital investigation and analysis techniques used for acquiring, validating, and analyzing electronic data to reconstruct events related to security incidents.	
Bit-Stream Copy/Image	Information System
Chain of Custody	Intrusion
Computer Forensics	Measures
Computer Security	Network Forensics
Cyber Incident Response Team	Network Monitoring
Digital Forensic Systems	Personally Identifiable Information (PII)
e-discovery	Phishing
Escalation Procedures	Reconstitution of System
Evidence Archival	Risk
Forensic Analysis	Risk Assessment
Forensic Labs	Risk Management
Incident Characterization	Sanitization
Incident Handling	Security Alerts
Incident Records	Security Incident
Incident Response	Spillage/Contamination
INFOCON	System Compromise
Information Assurance Posture	Threat Motivation
Information Security Policy	Unauthorized Access
Information Stakeholder	Vulnerability

2.4 Cyber Security Training and Awareness	
Refers to the 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. Training activities are designed to instruct workers about their security responsibilities and teach them about information security processes and procedures to ensure duties are performed optimally and securely within related environments. Awareness activities present essential information security concepts that are designed to affect user behavior.	
Awareness	IT Security Training Program
Certification	Learning Management System (LMS)
Computer Based Training (CBT)	Learning Objectives
Curriculum	Needs Assessment
End User Security Training	Role-Based Training
Essential Body of Knowledge	Testing
Instructional Systems Design (ISD)	Training
Instructor Led Training (ILT)	Web Based Training (WBT)
IT Security Awareness Program	

2.5 IT Systems Operations and Maintenance	
Refers to the ongoing application of principles, policies, and procedures to maintain, monitor, control, and protect IT infrastructure and the information residing on it during the operations phase of an IT system or application in production.	
Access Control	Security Data Analysis
Antivirus Software	Security Measures
Backup	Security Reporting
Baseline	System Hardening
Configuration Management	System Logs
Continuous Monitoring	System Monitoring
Insider Threat	Threat Analysis
Intrusion Detection System	Threat Monitoring
Intrusion Prevention System	Vulnerability Analysis
Patch Management	Vulnerability Scanning
Penetration Testing	

2.6 Network and Telecommunications Security

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 it resides. Examples of these practices include perimeter defense strategies, defense-in-depth strategies, and data encryption techniques.

- Access Control
- Authentication
- Blackberry
- Boundary Protection Services
- Communications Security (COMSEC)
- Configuration
- Controlled Interface
- Cryptosecurity
- Defense-in-Depth
- Emission Security
- Encryption Technologies (e.g., Secure Sockets Layer [SSL], Transport Layer Security [TLS])
- External Information Systems
- Firewall
- Hub
- Intrusion Detection System
- Intrusion Prevention Systems
- Load Balancers
- Network Architecture
- Networking Models and Protocols (i.e.: Open Systems Interconnection (OSI) or TCP/IP)
- Network Segmentation (e.g., Virtual Local Area Network [V-LAN], Demilitarized Zone [DMZ])
- Peer-to-Peer (P2P) Networking
- Penetration Testing
- Port
- Portable and Mobile Devices
- Protected Transmission/Distribution System
- Remote Access
- Router
- Security Trust
- Switch
- Telecommunications Technology (e.g., Private Branch Exchange [PBX] and Voice Over Internet Protocol [VOIP])
- TEMPEST
- Transmission Security
- Technical Surveillance Countermeasures (TSCM)
- Virtual Private Network (VPN)
- Vulnerability
- Web Services Security
- Wired and Wireless Networks

2.7 Personnel Security

Refers to methods and controls used to ensure that an organization's selection and application of human resources (both employee and contractor) are controlled to promote security. Personnel security controls are used to prevent and detect employee-caused security breaches such as theft, fraud, misuse of information, and noncompliance. Controls include organization/functional design elements such as separation of duties, job rotation, and classification.

- Access Authorization (Clearance)
- Background Checks/Background Investigation
- Confidentiality
- Digital Identity
- Human Resources
- Insider Threat
- Job Rotation
- Nondisclosure Agreement
- Position Sensitivity
- Screening
- Security Breach
- Security Clearance
- Separation of Duties
- Social Engineering
- Special Background Investigation (SBI)
- Suitability Determination

2.8 Physical and Environmental Security

Refers to methods and controls used to proactively protect an organization from natural or man-made threats to physical facilities and buildings, and to physical locations where IT equipment is located or work is performed (e.g., computer rooms, work locations). Physical and environmental security protects an organization's personnel, electronic equipment, and data/information.

Access Cards	Inventory
Access Control	Manmade Threat
Alarm	Natural Threat
Asset Disposal	Perimeter Defense
Biometrics	Protected Telecommunication/Distribution
Defense-in-Depth	Systems
Environmental Threat	Risk Management
Identification and Authentication	Threat and Vulnerability Assessment
	Video Surveillance

2.9 Procurement

Refers to the application of principles, policies, and procedures required to plan, apply, and evaluate the purchase of IT products or services—including "risk-based" pre-solicitation, solicitation, source selection, award, monitoring, disposal, and other post-award activities. Procurement activities may consist of the development of procurement and contract administration documents that include, but are not limited to, procurement plans, estimates, requests for information, requests for quotes, requests for proposals, statements of work, contracts, cost-benefit analyses, evaluation factors for award, source selection plans, incentive plans, SLAs, justifications required by policies or procedures, and contract administration plans.

Acceptable Risk	Request for Information
Acquisition	Request for Proposal (RFP)
Acquisition Life Cycle	Risk Analysis
Business Impact Analysis	Risk-Based Decision
Contract	Risk Mitigation
Cost-Benefit Analysis	Security Requirements
Disposal	Service Level Agreement (SLA)
Evaluated and Validated Products	Solicitation
Prequalification	Statement of Objectives (SOO)
Regulatory Compliance	Statement of Work (SOW)
	Supply Chain Risk
	Total Cost of Ownership (TCO)

2.10 Regulatory and Standards Compliance

2.10 Regulatory and Standards Compliance	
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.	
Accountability Accreditation Assessment Auditing Certification Compliance Ethics Evaluation Executive Orders FISMA Reporting Governance Laws (including but not limited to the Gramm-Leach-Bliley Act, Family Educational Rights and Privacy Act, Health Insurance Portability and Accountability Act [HIPAA], Federal Information Security Management Act [FISMA], Clinger-Cohen Act, Privacy Act, Sarbanes-Oxley, etc.)	National Institute of Standards and Technology (NIST) Special Publications Plan of Action and Milestones (POA&M) Policy Privacy Impact Assessment Privacy Principles/Fair Information Practices Procedure Regulations Security Program Standards (e.g., ISO 27000 series, Federal Information Processing Standards [FIPS]) Validation Verification

2.11 Security Risk Management

Refers to the policies, processes, procedures, and technologies used by an organization 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.

Acceptable Risk	Risk Mitigation
Accreditation Boundary	Risk Treatment
Annual Loss Expectancy	Security
Annual Rate of Occurrence	Security Controls
Asset Valuation	Security Measures
Benchmarking	Single Loss Expectancy
Business Impact Analysis	Supply Chain Risk
Consequence of Loss Determination	System Categorization
Design Basis Threat	Threat
Equivalency/Exemption	Threat and Vulnerability Assessment
Likelihood Determination	Threat Modeling
Logical Impacts	Types of Risk
Operational Impacts	Vulnerability
OPSEC/CI Threat	
Physical Environment Impacts	
Plan of Actions and Milestones (POA&M)	
Residual Risk	
Risk Analysis	
Risk Equation	
Risk Level	

2.12 Strategic Security Management

Refers to the principles, practices, and methods involved in making managerial decisions and actions that determine the long-term performance of an organization. Strategic security management requires the practice of external business analyses such as customer analyses, competitor analyses, market analyses, and industry environmental analyses. It also requires the performance of internal business analyses that address financial performance, performance measurement, quality assurance, risk management, and organizational capabilities/constraints. The goal of these analyses is to ensure that an organization's IT security principles, practices, and system design are in line with its mission statement.

Acquisition Management	Enterprise Security
Budgeting Process and Financial Management	Performance Management
Built-in Security	Strategic Planning
Capital Planning	Strategic Resource and Investment Mgmt.
Enterprise Architecture	Supply Chain Risk Management

2.13 System and Application Security	
Refers to principles, policies, and procedures pertaining to integrating information security into an IT system or application during the System Development Life Cycle (SDLC) prior to the Operations and Maintenance phase. The practice of these protocols ensures that the operation of IT systems and software does not present undue risk to the organization and its information assets. This objective is accomplished through risk assessment; risk mitigation; security control selection, implementation and evaluation; and software security standards compliance.	
Accreditation	Secure Coding Tools
Accreditation Boundary	Secure System Design Security Change Management
Application Controls	Security Requirements Analysis
Baseline Security	Security Specifications
Certification	Security Testing and Evaluation (ST&E)
Configuration Management	Security Vulnerability Analysis
Controlled Interface	Software Assurance
Form of Accreditation	Supply Chain Risk
Patch Management	System Categorization
Process Maturity	System Development Life Cycle (SDLC)
Risk Assessment	System Engineering
Risk Mitigation	Technical Security Controls
Secure Coding	
Secure Coding Principles	

Appendix 2. The Cyber Security Role-Based EBK: Competency and Functional Matrix

The following matrix, **Figure 1**, depicts the minimum required core competency training requirements for each cyber security key role. *Note: The shaded rows depict core competencies that are most common to all key cyber roles*.

Senior DOE Management can develop and/or require additional competency training for a specific key role based on operational needs of the organization. Additionally, it is recognized that individuals assigned these roles may have additional functional responsibilities. Senior DOE Management and/or Operating Units are responsible for identifying and providing any additional training for these key individuals to ensure that all functional roles are addressed.

Figure 2 depicts the correlation between the DOE-identified core competency training requirements and the seven high-level categories as identified by the National Initiative for Cybersecurity Education (NICE). Descriptions of the high-level categories are provided below.

1. **Securely Provision:** Specialty areas concerned with conceptualizing, designing, and building secure IT systems, with responsibility for systems' development. To include: Information Assurance Compliance, Software Engineering, Enterprise Architecture, Technology Demonstration, System Requirements Planning; Test and Evaluation, and System Development.

2. **Operate and Maintain:** Specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security. To include: Data Administration, Information System Security Management, Knowledge Management, Customer Service and Technical Support, Network Services, System Administration, and Systems Security Analysis.

3. **Protect and Defend:** Specialty areas responsible for the identification, analysis, and mitigation of threats to internal IT systems or networks. To include: Computer Network Defense, Incident Response, Computer Network Defense Infrastructure Support, Security Program Management, and Vulnerability Assessment and Management.

4. **Investigate:** Specialty areas responsible for the investigation of cyber events and/or crimes of IT systems, networks, and digital evidence. To include: Investigation and Digital Forensics.

5. **Collect and Operate:** Specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used

to develop intelligence. To include: Collection Operations, Cyber Operations Planning, and Cyber Operations.

6. **Analyze:** Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence. To include: Cyber Threat Analysis, Exploitation Analysis, All source Intelligence, and Targets.

7. **Oversight and Development:** Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work. To include: Legal Advice and Advocacy, Strategic Planning and Policy Development, and Education and Training, Information Systems Security Operations, and Security Program Management.

Figure 1: DOE Cyber Security Role, Competency, and Functional Matrix

DOE Cyber Security EBK: A Competency and Functional Framework for Cyber Security Workforce Development		DOE Cyber Security Functional Roles											
		Chief Information Officer (CIO)	Information Owner/Steward	Chief Information Security Officer (CISO)	Authorizing Official (AO)	AO Designated Representative (AODR)	Common Control Provider	Information System Owner	Cyber Security Program Manager (CSPM)	Information System Security Officer (ISSO)	Information Security Architect	Information System Security Engineer	Security Control Assessor
Core Competencies	Data Security		•	•		•	•	•	•	•	•	•	•
	Enterprise Continuity		•	•	•	•	•	•	•	•	•	•	•
	Incident Management		•	•	•	•	•	•	•	•	•	•	•
	Cyber Security Training and Awareness			•	•	•		•	•	•			•
	IT Systems Operations and Maintenance		•	•		•	•	•	•	•		•	•
	Network and Telecommunications Security and Remote Access			•		•	•	•	•	•	•	•	•
	Personnel Security			•				•	•	•			•
	Physical and Environmental Security			•				•	•	•			•
	Procurement							•		•			
	Regulatory and Standards Compliance			•	•	•		•	•	•			•
	Security Risk Management (RMA)	•	•	•	•	•	•	•	•	•	•	•	•
	Strategic Security Management			•	•			•	•				•
	System and Application Security (*System Authorization*)		•	•	•	•	•	•	•	•	•	•	•

Figure 2: NICE Cybersecurity Workforce Framework High-Level Categories Cross-reference to DOE Cyber Security Role, Competency, and Functional Matrix

NICE Cybersecurity Workforce Framework Categories	DOE Cyber Security Key Functional Roles													
	Correlation between NICE Cybersecurity Framework and DOE Cyber Security Key Functional Roles	**Data Security**	**Enterprise Continuity**	**Incident Mgmt.**	**Cyber Security Training & Awareness**	**IT Systems Operations & Maintenance**	**Network & Telecomm Security & Remote Access**	**Personnel Security**	**Physical & Environmental Security**	**Procurement**	**Regulatory & Standards Compliance**	**Security Risk Mgmt.**	**Strategic Security Mgmt.**	**System & Application Security**
	Securely Provision	•									•	•	•	•
	Operate & Maintain	•			•	•	•			•				•
	Protect & Defend	•	•	•				•	•			•	•	•
	Investigate			•										
	Collect & Operate			•									•	
	Analyze			•								•	•	
	Oversight & Development			•	•					•	•	•	•	•

Appendix 3: List of Acronyms

Acronym	Definition
A	
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
B	
BIA	Business Impact Analysis
C	
CA	Certification Agent
C&A	Certification and Accreditation
CBT	Computer Based Training
CIO	Chief Information Officer
CIRC	Cyber Incident Response Capability
CISO	Chief Information Security Officer
CMP	Configuration Management Plan
CNSS	Committee on National Security Systems
COMSEC	Communications Security
CSAT	Cyber Security Awareness and Training
CSPM	Cyber Security Program Manager
CSTW	Cyber Security Training Warehouse
D	
DAA	Designated Approval Authority
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
E	
EBK	Essential Body of Knowledge
EISA	Enterprise Information Security Architecture
F	

Acronym	Definition
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
H	
HIPAA	Health Insurance Portability and Accountability Act
I	
IA	Information Assurance
ILT	Instructor Led Training
ISO	International Standards Organization
ISSLoB	Information Systems Security Line of Business
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
ITSC-WG	Information Technology Security Certification Working Group
ST&E	Security Testing and Evaluation
L	
LMS	Learning Management System
N	
NCSD	National Cyber Security Division
NIST	National Institute of Standards and Technology
NSS	National Security System
O	
OMB	Office of Management and Budget
OCIO	Office of the Chief Information Officer
P	
P2P	Peer-to-Peer Networking
PBX	Private Branch Exchange
PCSP	Program Cyber Security Plan
PIA	Privacy Impact Assessment

Acronym	Definition
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
R	
RFP	Request for Proposal
RMIP	Risk Management Implementation Plan
ROI	Return on Investment
S	
SDLC	System Development Life Cycle
SLA	Service Level Agreement
SME	Subject Matter Expert
SOW	Statement of Work
SSE CMM	Systems Security Engineering Capability Maturity Model
SSL	Secure Sockets Layer
SUI	Sensitive Unclassified Information
T	
TMR	Technical and Management Requirements
U	
US-Cert	United States Computer Emergency Readiness Team
V	
V-LAN	Virtual Local Area Network
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Network
W	
WBT	Web Based Training