U.S. DEPARTMENT OF ENERGY

Cyber Security Awareness and Training Program Plan and 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 2009

Table of Contents

Executive Summary

The Department of Energy (DOE) Cyber Security Awareness and Training (CSAT) program provides the Department the opportunity to leverage its greatest assets – People. By providing a comprehensive approach to training and awareness, CSAT ensures all levels of Departmental personnel are informed of their cyber security responsibilities and possess skills appropriate to their functional roles to adequately protect Government electronic information and information systems. The program design is led by a strategy that reaches beyond the confines of the training function itself to ensure a meaningful contribution to the Cyber Security Strategy and mission goals of the Department. It defines minimum training requirements and supplies DOE-specific curriculum that can be utilized by Senior DOE Management to provide user and role-based training.

The CSAT curriculum is designed in four focus areas that address cyber security responsibilities applicable to all staff in relation to their job functions.

- User Awareness
- User Training
- Role-based Training for staff with significant cyber security responsibilities
- Education and Certification for cyber security professionals

The Office of the Chief Information Officer (OCIO) utilized DOE cyber security policy, best practices and lessons learned, and comprehensive internal needs assessments to identify fundamental cyber security functional roles and associated responsibilities and define the essential body of knowledge (EBK) needed to support cyber security responsibilities and activities within the Department. Components of the EBK are assigned to each functional role, and customized curriculum is determined for each key role. The key functional roles, as defined in DOE M 205.1-5, *Cyber Security Process Requirements Manual,* are: Cyber Security Program Manager (CSPM), Designated Approval Authority (DAA), Designated Approving Authority Representative (DAAR), Information Systems Security Manager (ISSM), Certification Agent (CA), System Owner, , and the Information System Security Officer (ISSO).

The EBK accomplishes two important Departmental training goals: 1) defining the baseline knowledge, skills, and abilities required for 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 are fit into the specific curriculum for each of the Department-defined 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 delivered through a variety of methods, including classroom instruction, workshop/seminar, and online options and can be tailored to Basic, Intermediate, and Advanced levels.

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 800-16 and 800-50 guidance, and address the functional roles and responsibilities discussed in Departmental cyber security Directives. The modules and courses may be used by Senior DOE Management or Operating Unit Managers as a base for supplemental Senior DOE Management[1] Program Cyber Security Plans (PCSPs) or organization-specific training.

The CSAT program also includes the Cyber Security Training Warehouse (CSTW), a web-based resource that provides direct access to training and awareness resources, program documents, and current DOE cyber security policy and guidance. The CSTW will provide a centralized Learning Management System (LMS) and Performance Reporting element for evaluation and control of the program, including monitoring of feedback for program logistics, delivery, content, and curriculum.

1.1 Purpose

This document describes the immediate and long-term plan for the DOE CSAT program, including identifying requirements, and developing and delivering training offerings that focus on performance. The plan is a blueprint for creating the training required to support the Department's cyber security goals and provide staff with professional growth opportunities. The output of the program outlined in this plan answers the following questions:

- Who needs to be trained?
- What are the training objectives and high-level content for each audience?
- When and where the training should occur?
- How should they be trained?
- How will training materials be developed/acquired and implemented?

The process that has been undertaken to develop the core elements of the program are documented in the Draft Cyber Security Awareness & Training Strategic Approach, dated January 2008.

1.2 Background

1.2.1 National Requirements

The *Computer Security Act of 1987* requires mandatory periodic training in cyber security awareness and accepted cyber security practice for all employees involved with the management, use, or operation of a Federal computer system under Government supervision. This training requirement includes contractors.

[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

Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Information Systems*, requires individuals using general support systems or major applications to be trained on security responsibilities prior to initial system access.

The *Federal Information Security Management Act* mandates general training of employees to ensure that they are aware of their security responsibilities, specialized training of agency employees with significant security responsibilities, and reporting of Agency statistics on security awareness and training efforts.

Title 5, Code of Federal Regulations, Subpart C, *Employees Responsible for the Management or Use of Federal Computer Systems*, sections 930.302 through 930.305 addresses training requirements for Federal employees.

HSPD-7, *Critical Infrastructure Protection*, specifies “there shall be Vulnerability Awareness and Education Programs within both the government and the private sector to sensitize people regarding the importance of security and to train them in security standards, particularly regarding cyber systems.”

The Committee on National Security Systems (CNSS) Directive 500 mandates training and awareness activities for all Federal and contractor employees who access, operate, manage, maintain, secure, develop, or acquire a National Security System (NSS) appropriate to the level of knowledge, experience, and responsibilities of the employee.

National Security Telecommunications and Information Systems Security Directive Number 501, *National Training Program for Information Systems Security (INFOSEC) Professionals*, requires the implementation of an Agency-specific INFOSEC training program that includes a common body of knowledge for INFOSEC professionals. Contractors must comply with the directive when they are responsible for the security oversight or management of NSS operated on behalf of the Federal Government.

1.2.2 Department of Energy

The baseline Departmental cyber security requirements are defined in the DOE Cyber Security Directives and OCIO guidance and reference documents, including the following.

- DOE O 205.1A, *Department of Energy Cyber Security Management*, 12/04/2006
- DOE M 205.1-4, *National Security System Manual*, 03/08/2007
- DOE M 205.1-5, *Cyber Security Process Requirements Manual*, 08/12/2008
- DOE M 205.1-6, *Media Sanitization Manual*, 12/23/2008
- DOE M 205.1-7, *Security Controls for Unclassified Information Systems Manual*, 01/05/09
- DOE M 205.1-8, *Cyber Security Incident Management Manual*, 01/08/09

The following additional documents also provide the Department-specific foundation for content and direction of the CSAT program.

- Cyber Security Strategic Plan
- The Annual Cyber Security Action Plan
- DOE Enterprise Architecture
- DOE Capital Planning Investment Control Guide

1.2.3 Information System Security Lines of Business (ISSLoB)

In March 2004, the Office of Management and Budget (OMB) initiated a Government-wide analysis of five lines of business (LoBs) supporting the President's Management Agenda goal to expand Electronic Government. In March 2005, OMB kicked off an Information System Security LoB (ISSLoB) task force focused on a number of cyber security-based initiatives including the conduct of training, awareness, and knowledge sharing. Under ISSLoB Tier I training, OMB defined a common framework for general awareness to be used as mandatory annual cyber security refresher briefings across the Government and required Agencies to select a Shared Service Provider (SSP) to deliver the common refresher content. Similarly, ISSLoB Tier II training will provide universal content and SSPs for role-based training.

The CSAT program complies with ISSLoB content requirements and, where possible, leverages ISSLoB services to address DOE and Federal requirements for cyber security training and education. Under the ISSLoB, the Department selected Defense Information Systems Agency (DISA) as the provider for delivery of Security Awareness Training (Tier I). By agreement, DISA is responsible for product development, including collecting requirements, developing and managing content, and delivering a product for Departmental implementation. All ISSLoB content requirements are incorporated in the DOE EBK.

1.3 CSAT Program Overview

The Department’s information systems are attacked tens of thousands of times a day; 24 hours a day; 365 days a year. These attacks originate from many locations across the globe and use an increasingly sophisticated and varied range of techniques and technologies to attempt to gain unauthorized access to DOE assets or deny others access to those systems. Effective protection of the Department’s information systems and data assets are critical to the continued success in the four key mission areas: 1) national security; 2) environmental quality; 3) science and technology; and 4) energy resources.

Overall authority and responsibility for securing DOE information and information technology assets rests with the Secretary of Energy. Under FISMA, the Chief Information Officer (CIO) has the responsibility to develop cyber security policies and ensure the training of Departmental personnel in the requirements of these Directives. The cyber security governance structure defined in DOE O 205.1A, *Department of Energy Cyber Security Management*, requires that Senior DOE Management develop, implement, and maintain training programs for their Operating Units through their respective PCSPs.

1.3.1 Vision and Mission

The vision of the CSAT program is to ensure that all Departmental personnel and contractors are aware of and trained to execute their cyber security responsibilities and DOE requirements to protect the confidentiality, integrity, and availability of information and information systems.

The CSAT mission is to provide a core body of knowledge, role-based curriculum, and enterprise resources for cyber security awareness, training/education, and professional development that are available to all Department organizations and personnel.

1.3.2 Objectives

The DOE CSAT program has the following major objectives:

- Define a baseline EBK,
- Define competencies, requirements, and training objectives for Department-defined functional roles, and
- Provide training and awareness activities and materials with emphasis on the importance of security, standards, cyber security responsibilities, and support for the competencies identified in the EBK.

1.4 Departmental CSAT Components

To protect information systems, all users must have timely, relevant, and easily accessible information that will raise awareness about cyber risks, vulnerabilities, and requirements. Cyber security staff must also develop skills for protection of information and information systems appropriate to their functional responsibilities. This CSAT program targets DOE Federal and contractor personnel in distinct job functions and links each with unique security skills and accurate, current security information. The key functional roles, as defined in DOE M 205.1-5, *Cyber Security Process Requirements Manual*, are: Cyber Security Program Manager (CSPM), Designated Approval Authority (DAA), Designated Approving Authority Representative (DAAR), Information Systems Security Manager (ISSM), Certification Agent (CA), System Owner, and the Information System Security Officer (ISSO). This CSAT program also addresses the DOE General User. Although General User is not listed as a key functional role, it is understood that a well-educated workforce is critical in securing DOE information and information assets. Therefore, a General User EBK has been developed to assist Senior DOE Management and Operating Unit organizations with developing a comprehensive General User Awareness and Training Program that includes knowledge and skills beyond the annual refresher briefing.

Under the governance model described in DOE O 205.1A, *Department of Energy Cyber Security Management*, Senior DOE Management organizations are responsible for providing cyber security training to their Operating Units. The CSAT program builds the Departmental policy and requirements to ensure a consistent baseline of instructional content that meets the needs of the cyber security community as well as Federal requirements. In addition, the program is a training service provider to Departmental Elements, delivering courseware and training opportunities that fulfill the requirements defined in the policy. CSAT activities include:

- An update of Departmental Directives to include cyber security training and awareness as a segment of Senior DOE Management PCSPs;
- Definition of core knowledge, skills, and abilities for functional cyber security roles;
- Awareness materials and user training;
- Role-based training courseware for all cyber security personnel or practitioners;
- Technical and Management Training, to include comprehensive course offerings compliant with the DOE EBK and a repository of training resources, courses, and modules;
- A metrics program to assess the effectiveness of Department-wide and Operating Unit training programs;
- Participation in conferences and workshops to support community, disseminate information, and provide for continuing education units; and
- Incentive and recognition program.

By defining cyber security competencies, the EBK provides the foundation for defining the knowledge, skills, and abilities necessary for functional cyber security roles, assessing commercially and Federally available training products, and constructing DOE-specific modules. The CSAT curriculum and the delivery model provides for role-based training to those with significant cyber security responsibilities (e.g. DAA, CSPM, ISSM, CA, system owner, ISSO) and makes available training from existing courses for those who have significant management responsibilities that interleave with cyber security (e.g. General Counsel, Inspector General, Contracting Officer, Contracting Officer Technical Representative). The program includes a variety of courses and delivery methods. The core of the technical training, which is either developed in-house or commercially procured, is high-quality, diligently developed and maintained, and readily available and can be supplemented to meet organizational requirements.

1.4.1 Cyber Security Awareness and Training Directive

The OCIO is responsible for promulgating a Departmental Directive that defines the DOE cyber security awareness and training program and formalizes the responsibilities for administering cyber security training within the Department. The Directive for DOE Cyber Security Awareness and Training will also include requirements for the following:

- A Department-wide awareness and training program and infrastructure;

- Definition of an essential body of knowledge (EBK), skills, and abilities for role-based cyber security training;
- Adherence to Federal training requirements;
- Conduct of training for all defined roles, including Operating Unit specialized training; and
- An annual program review.

1.4.2 DOE Essential Body of Knowledge (EBK)

The Department's workforce must be prepared to meet the cyber security challenges that exist today and will evolve in the future. Cyber security is a strategic priority that ensures mission achievement. The EBK accomplishes two important Departmental training goals: 1) defining the baseline knowledge, skills, and abilities required for cyber security functional roles, and 2) providing the foundational objectives for the development, selection, and presentation of training.

As stated previously, DOE has designated the following to be key functional roles: CSPM, DAA, DAAR, ISSM, CA, system owner, and ISSO. However, it is recognized that individuals assigned these roles may have additional functional responsibilities based on the needs of a specific Operating Unit. Senior DOE Management and/or Operating Units are responsible for identifying and providing any additional training for these key individuals to ensure that all functions are addressed. For example, if a DAA is primarily responsible for all DAAR functions, then he/she will have to be adequately trained in core competencies as identified in this document for both key roles.

To meet the goal of training and awareness for all Departmental employees, the DOE EBK has two suites of competencies: one specific to general users and one specific to functional roles with significant cyber security responsibilities. The primary distinction between the two suites is the level of technical detail necessary to execute cyber security responsibilities.

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* is a competency-based framework that links specific knowledge, skills, and abilities to functional cyber security roles. Both suites of the Departmental EBK use this document as a foundation; they also incorporate other established bodies of knowledge and managerial, technical, assurance, and operational concepts and requirements of the DOE Directives and OCIO reference baselines.

The EBK identifies the core cyber security competencies (i.e., knowledge, skills, and abilities) in which all Departmental staff are expected to be proficient and is the foundation of a standard training and education curriculum for all functional roles. Additionally, the EBK includes a matrix of required competencies by functional role. The EBK is one of the components necessary for a comprehensive training program and is to be supplemented with Senior DOE Management and local training requirements.

The EBK also guides the CSAT curriculum development, course design, and implementation activities; is a template for assessing relevance of training resources (commercial and Governmental) available to the Department; and provides a documented foundation with respect to pending legislation in professional standards. The EBK approach provides the benefits of:

- Articulating the function roles performed by Departmental staff,
- Defining minimum awareness criteria,
- Promoting uniform competency requirements to increase the overall efficacy of cyber security role-based training,
- Providing a flexible set of minimum competencies that can be tailored with local policy and procedure requirements, and
- Providing foundational content requirements that can be leveraged to facilitate professional development of the cyber workforce, including future training and education, academic curricula, or affiliated human resource activities.

It is recognized that there are many equally effective ways to organize a curriculum; the EBK specifies a minimum set of subject matter that is required for all role-based training programs. All program courseware will exhibit the recommended core material and/or provide supplemental material related to the overall course content.

The DOE EBK utilizes the same terms; concepts; and “manage,” “design,” “implement,” and “evaluate” perspectives and customizes the 13 competency areas of the NCSD EBK. The DOE EBK includes an assessment of each competency perspective as it applies to the nine functional roles; the resulting matrix provides the foundation for specifying customized curriculum for each functional role. The 13 NCSD EBK competencies are:

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

1.5 The Cyber Security Warehouse

To support its role as a training service provider, the CSAT Program offers an online repository, the Cyber Security Training Warehouse (CSTW), that provides direct access to training and awareness resources, program documents, and current DOE cyber security policy and guidance. The CSTW will provide links for e-learning, course registration, workshop presentations, performance reporting, policies and procedures, and professional development. At initiation, the Warehouse will provide access to the following resources.

- **Awareness & Communication** – awareness campaign materials including newsletters, brochures, and pre-configured campaign print materials including banners, posters, and leaflets that can be modified for local use. The site references up-to-date information regarding enterprise awareness initiatives, including the topic of the quarter, best practices for implementation, and materials to support awareness campaigns at Departmental sites.

- **Training & Education** – information on training curriculum and opportunities, including a description of the modules, resources, and scheduled courses, as well as a link to the DOE Online Learning Center (OLC^2). This page will also include the CSAT-available curriculum for each role identified in the EBK and provide a crosswalk of requirements to commercially available training resources, such as SANS Institute. This page also includes information on accessing commercial training programs available through DOE and the OCIO.

- **Professional Development –** reference material and links to cyber security professional associations and certifying organizations and undergraduate/graduate programs specializing in degree-based curriculum leading to a Bachelors or Masters degree in Information Security.

- **Resources –** links to Federal and Department requirements and guidance governing the practices of the DOE Cyber Security Program.

- **Conferences, Workshops and Training Schedules** – master schedule of DOE-sponsored training and information-exchange opportunities. This page also provides links to register for Departmental cyber security events, such as seminars, workshops, and the annual conference.

1.6 The CSAT Curriculum

A key service provider component of the CSAT program is the delivery of training curriculum, materials, and courseware addressing the competencies defined in the DOE EBK and the requirements outlined in OMB A-130 and the ISSLoB. The courseware catalog includes commercial and DOE-developed modules linked to Federal requirements and EBK competencies and presented through a myriad of resources including instructor-led classes; computer-based and online training, and self-paced instructional services.

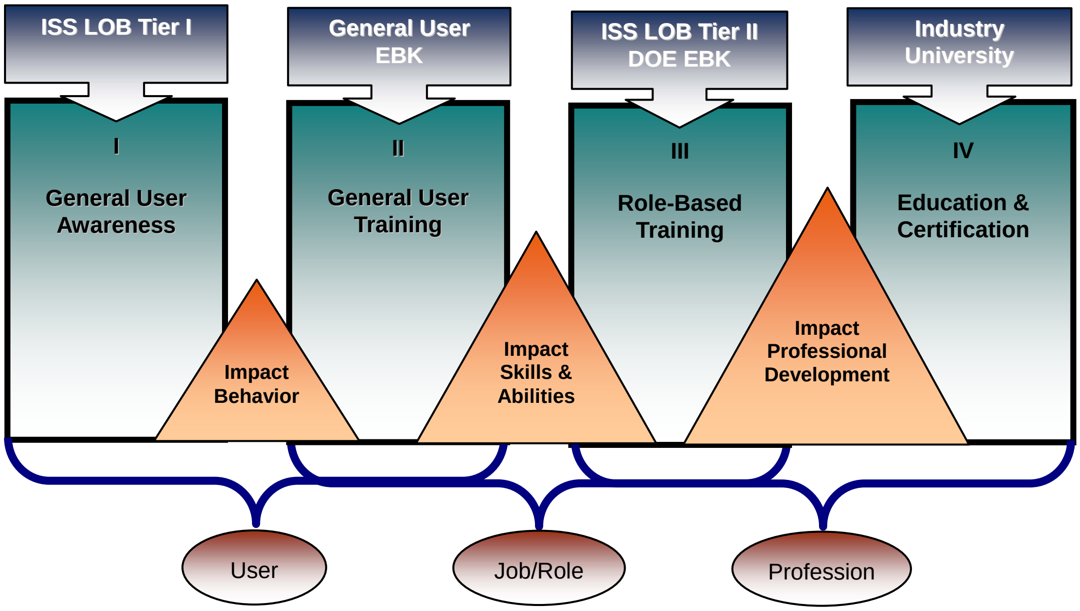
The curriculum applies to four main areas of cyber security training.

- User Awareness
- User Training

- Role-based Training for staff with significant cyber security responsibilities
- Education and Certification for cyber security professionals

Figure 1 depicts the correlation of these focus areas to each other, their functional applicability, and the underlying requirement.

Figure 1, Cyber Security Curriculum Foundation in Context



1.6.1 General User Awareness

Cyber security awareness programs impress upon users the importance of cyber security and the adverse consequences of its failure. The purpose of awareness activities is to focus attention on security. Awareness relies on using attractive packaging techniques to reach broad audiences. Although more informal in nature, it is important to set the stage for security training for both users and security professionals. Awareness activities lead users to understand their roles and responsibilities related to organizational mission; understand cyber security policy, procedures, and practices; and ensure a fundamental knowledge of management, operational, and technical controls required to protect the information for which they are responsible. Awareness may reinforce knowledge already gained, but its goal is to produce security behaviors that are automatic and consistent.

Annual Cyber Security Awareness Training

General user awareness training must be completed by each Departmental employee (including contractors) at least annually. The CSAT will provide a basic Department-level refresher briefing to Senior DOE Management every year for dissemination to all Operating Units; this briefing can and should be augmented to include current Senior

DOE Management and Operating Unit policies and procedures. The content of the briefing will be updated annually to reflect any changes in responsibilities or processes described for users in the DOE Directives, the DOE EBK, and the ISSLoB. It is the intent of the CSAT program to provide centralized delivery of the annual refresher briefing, when it becomes technically feasible; until then a common baseline briefing will be disseminated for local execution.

Awareness Campaigns and Materials

Cyber security awareness programs impress upon users the importance of cyber security and the adverse consequences of its failure. Awareness may reinforce knowledge already gained, but its goal is to produce security behaviors that are automatic. Awareness activities can build in these behaviors for the security professional and the everyday user. The CSAT program is the focal point for the development of quarterly awareness campaigns targeted for the DOE general audience. Campaign topics are set at the beginning of each calendar year with the approval of the Associate Chief Information Officer for Cyber Security. The campaigns include, but are not limited to:

- Special-interest organized activities, such as seminars, guest speakers, etc.
- Posters
- Newsletters
- Informational e-Mails
- Promotional materials

Special emphasis is placed on “Cyber Security Awareness Day” program and activities, an annual day-long event that features special events and programs targeted at general users and security professionals.

Awareness campaigns are piloted at the DOE Headquarters and resource toolkits for each are prepared and posted to the CSTW for use throughout the Department. Logistics for the campaign events are provided under the Communications and Outreach Program of the Office of Cyber Security.

Conferences and Workshops

OCIO-sponsored conference and workshops provide opportunities for delivery of cyber security training. Resources from the CSAT program are provided as appropriate. Participation in these activities is managed under the Communications and Outreach Program of the Office of Cyber Security.

1.6.2 Training Curriculum

The two center blocks of Figure 1 depict the two-level structure of the training component of this program. Training is more formal, having a goal of building knowledge and skills to facilitate job performance. Certainly, General Users do not require the level of information needed by a staff in functional roles with significant security responsibilities. A General User Essential Body of Knowledge consisting generic concepts, terms, and associated learning models, as well as procedural specifics, guides the development of this type of transitional activity between awareness and professional-level training. This training represents a baseline of cyber security knowledge that all employees can reasonably be expected to have – basically, “what to know” and “what to do” in relation to safe computing practices.

Different levels of training are required for individuals whose role in the organization indicates a need for special knowledge of cyber security threats, vulnerabilities, and safeguards; this training is focused on functional responsibilities and develops the skills needed to execute them successfully. These courses are provided to individuals that are responsible for ensuring the security of all DOE information systems. Through role-based training, all personnel involved in the management, use, design, development, maintenance or operation of an application or automated information system are made aware of their security responsibilities based on their level of access to systems and data (need-to-know), trained to fulfill them, and versed in the rules and requirements pertaining to security of the Federal IT systems they access, operate, or manage.

Training Resources

It is not viable or advantageous for the Department to create new training courseware for all competencies identified from the EBK. The Department already has access to commercial, Federal, and other training resources that may fulfill the requirements and objectives of the training program. This activity begins with documenting the content of available courseware against the competencies defined in the EBK with known resources, such as the Online Learning Center (OLC2) and SANS Institute, as well as classes already being offered by the OCIO. Additional training resources will be identified, first through contact within the Department, and reviewed against the EBK to determine how they can be leveraged to fulfill training requirements. As part of this activity, any training gaps will be identified that require in-house course/module development or procurement of additional commercial or Federal training resources.

Function Role Curriculum

Using the cross-walked competency chart from the EBK and the identified resources, a curriculum of specific courses/modules from existing resources will be identified for each functional role. The curriculum will be posted to the CSTW.

1.6.3 Courseware Development

As much as possible, the CSAT will leverage available courseware to meet the requirements defined in the EBK. In some cases, it may be advantageous or necessary to develop courseware. A continuous assessment of available courseware products is necessary to ensure that training for EBK competencies is available and appropriate. When gaps are identified, a “market survey” and cost analysis is done to determine if courseware can be obtained that is appropriate and cost-efficient.

If it is determined that a course development activity is required, key components under each gap-applicable competency of the EBK are compiled into outlines for draft training module(s) and evaluated against manage, design, implement, and evaluate perspectives. The draft module will identify the competencies supported, module objectives, and the content necessary to support those objectives. Requirements for designing modules for basic, intermediate, and advanced presentation, as well as modifications that may be required for each cyber security functional role, will also be annotated at this time. This emphasis on roles, rather than on fixed content, gives the CSAT Program requirements flexibility, adaptability, and longevity.

All DOE-developed courseware will be completed and piloted prior to being incorporated into any functional role curriculum.

1.6.4 Performance Monitoring and Reporting

Currently, there is no mechanism to centrally manage student participation with the courseware identified under the CSAT. In addition, the DOE cyber security governance model does not require the use of training resources identified or provided by the OCIO. When technically feasible, a centralized learning management system will be put in place to track usage of CSAT resources. In the interim, CSAT will assess program participation through class rosters and feedback, update resources as needed, and provide available usage statistics to Senior DOE Management as appropriate.

Appendix 1: DOE Cyber Security Role-Based Essential Body of Knowledge

Information and system security is by its nature multidisciplinary, and it relies on a spectrum of knowledge and performance items/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/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 Program Cyber Security Plans (PCSP)

- 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, 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/PCSP 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 PCSPs
- 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)
- 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/PCSP 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
- 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 PCSPs
- 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). 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., 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 take~~s~~ 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 CIRC
- Identify services that the incident response team should provide
- Create an Incident Response Management Plan in accordance with DOE policies and the applicable PCSP
- Develop procedures for performing incident and INFOCON responses and maintaining records
- Develop procedures for handing information and cyber alerts disseminated by the DOE 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 DOE 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 DOE 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 DOE 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 DOE 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/PCSP 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 DOE 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 PCSP 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 PCSPs.

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 PCSPs
- 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/PCSP 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 PCSP 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/PCSP 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/PCSP 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/PCSP 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/PCSP 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/PCSP 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/PCSP 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 PCSPs

1.6.2 Design

- Develop network and host-based security policies in accordance with Departmental/PCSP standards, procedures, directives, policies, and regulations and laws (statutes)
- Specify strategic security plans for network telecommunications in accordance with Departmental/PCSP 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 PCSPs
- 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 PCSPs
- 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 PCSPs
- 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 PCSPs
- Implement policies and procedures related to P2P networking in accordance with Departmental directives and applicable PCSPs.

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/PCSP 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/PCSP 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/PCSP 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
- 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 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/PCSP 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/PCSP 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, 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
- 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/PCSP 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

- 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 PCSP
- 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
- 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/PCSP 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/PCSP 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 PCSPs
- 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 PCSP

1.13.3 Implement

- Execute the Departmental/PCSP 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

- 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/PCSP 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/PCSP 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 2: Cyber Security Role-Based EBK: Key Terms and Concepts

The purpose of this listing is to provide a basic understanding of key terms and concepts rather than offer an exhaustive list. Knowledge of these terms and concepts is the foundation for effective performance of functions associated with each of the technical competency areas.

The EBK lists all the key terms and concepts that have been identified for each competency area. At minimum, individuals should know, understand, and be able to apply those that relate to the competencies to which their role is linked. Full knowledge of all of the terms and concepts is the foundation for performance as a conversant IT security generalist. This section describes and lists the 13 IT security competency areas and their affiliated key terms and concepts.

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
Access Control
Aggregation
Antivirus Software
Authentication
Authorization
Categorize information & system
Consequence of Loss
Data Classification
Decryption
Digital Signatures
Discretionary Access Control
Electronic Commerce
Encryption
Firewall Configuration
Identity Data and Access Management
Identity Management
Information Classification Scheme
Least Privilege
Mandatory Access Control
Need-to-Know
Nonrepudiation
Personally Identifiable Information
Privacy
Privilege Levels
Protection Index
Public Key Infrastructure
Role-Based Access Control
Rule-Based Access Control
Sanitization
Secure Data Handling
Security Clearance
Sensitive Unclassified Information
Sensitivity Determination
Sensitivity of Data
Steganography
System High
System of Record
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
Backup Strategy
Business Continuity Plan
Business Impact Analysis
Business Recovery Plan
Contingency Plan
Crisis Communication
Critical Infrastructure
Cyber Incident Response
Delegation of Authority
Disaster Recovery
Disruption
Essential Functions
Information Technology Contingency Plan
Interoperable Communications
Key Resources
Mission Assurance
Occupant Emergency Plan
Order of Succession
Preparedness/Readiness
Risk Mitigation
Standard Operating Procedures
Test, Training, and Exercise
Threat Environment
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
Chain of Custody
Computer Forensics
Computer Security
Cyber Incident Response Team
Digital Forensic Systems
e-discovery
Escalation Procedures
Evidence Archival
Forensic Analysis
Forensic Labs
Incident Characterization
Incident Handling
Incident Records
Incident Response
INFOCON
Information Assurance Posture
Information Security Policy
Information Stakeholder
Information System
Intrusion
Measures
Network Forensics
Network Monitoring
Personally Identifiable Information (PII)
Phishing
Reconstitution of System
Risk
Risk Assessment
Risk Management
Sanitization
Security Alerts
Security Incident
Spillage/Contamination
System Compromise
Threat Motivation
Unauthorized Access
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
Certification
Computer Based Training (CBT)
Curriculum
End User Security Training
Essential Body of Knowledge
Instructional Systems Design (ISD)
Instructor Led Training (ILT)
IT Security Awareness Program
IT Security Training Program
Learning Management System (LMS)
Learning Objectives
Needs Assessment
Role-Based Training
Testing
Training
Web Based Training (WBT)

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
Antivirus Software
Backup
Baseline
Configuration Management
Continuous Monitoring
Insider Threat
Intrusion Detection System
Intrusion Prevention System
Patch Management
Penetration Testing
Security Data Analysis
Security Measures
Security Reporting
System Hardening
System Logs
System Monitoring
Threat Analysis
Threat Monitoring
Vulnerability Analysis
Vulnerability Scanning

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.

2.7 Personnel Security

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

2.9 Procurement

Acceptable Risk
Acquisition
Acquisition Life Cycle
Business Impact Analysis
Contract
Cost-Benefit Analysis
Disposal
Evaluated and Validated Products
Prequalification
Regulatory Compliance

Request for Information
Request for Proposal (RFP)
Risk Analysis
Risk-Based Decision
Risk Mitigation
Security Requirements
Service Level Agreement (SLA)
Solicitation
Statement of Objectives (SOO)
Statement of Work (SOW)
Total Cost of Ownership (TCO)

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

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
Budgeting Process and Financial Management
Built-in Security
Capital Planning
Enterprise Architecture
Enterprise Security
Performance Management
Strategic Planning
Strategic Resource and Investment 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
Accreditation Boundary
Application Controls
Baseline Security
Certification
Configuration Management
Controlled Interface
Form of Accreditation
Patch Management
Process Maturity
Risk Assessment
Risk Mitigation
Secure Coding
Secure Coding Principles
Secure Coding Tools
Secure System Design Security Change Management
Security Requirements Analysis
Security Specifications
Security Testing and Evaluation (ST&E)
Security Vulnerability Analysis
Software Assurance
System Categorization
System Development Life Cycle (SDLC)
System Engineering
Technical Security Controls

Appendix 3. The Cyber Security Role-Based EBK: Competency and Functional Matrix

The following matrix, Figure 2, provides a visual representation of the linkage between roles, competency areas, and work functions categorized as Manage, Design, Implement, or Evaluate in the EBK.

If a core competency and corresponding work function has been identified as a minimum training requirement for a key functional role, then the responsible work function will be denoted in the matrix as follows.

- M – Manage
- D – Design
- I – Implement
- E – Evaluate

The following matrix depicts the minimum training requirements for core competencies as determined for each key role defined in DOE M 205.1-5. It is important to note that not all activities listed within a work function apply to a given functional role. For example, while there may be some overlap, the Evaluate responsibilities for the CSPM, DAAR, ISSM, and CA are different; these differences must be considered when role-specific curriculum is designed.

Senior DOE Management can develop/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: 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 Key Functional Roles						
		Cyber Security Program Manager (CSPM)	Designated Approving Authority (DAA)	Designated Approving Authority Representative (DAAR)	Information System Security Manager (ISSM)	Certification Agent (CA)	System Owner	Information System Security Officer (ISSO)
Core Competencies	Data Security	M,E		E	M,D,E	I,E	D	I
	Enterprise Continuity				M	E		
	Incident Management	D	I		M,D			I
	Cyber Security Training and Awareness	M,D,E			M,D,I,E			I
	IT Systems Operations and Maintenance			E	M,D,E	E	D,I	I
	Network and Telecommunications Security and Remote Access			E	M,D,E	E	D,I	I
	Personnel Security				M,D		D	I
	Physical and Environmental Security				M,D		D	I
	Procurement						M	
	Regulatory and Standards Compliance	M,D,I,E		E	M,D,I,E	I,E		I
	Security Risk Management	M,D,E	E	I,E	M,D,E	I,E	D	D,I
	Strategic Security Management	M,D,I,E	M		M,D,I,E			
	System and Application Security		I	E	M,D,E	M,I,E	D,I	D,I

Appendix 4: List of Acronyms

Acronym	Definition
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	
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
H	

Acronym	Definition
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
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
R	

Acronym	Definition
RFP	Request for Proposal
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