NIST Special Publication 800-16
Revision 1 (2nd Draft, Version 2)

A Role-Based Model for Federal Information Technology/ Cyber Security Training

Patricia Toth
Penny Klein

I N F O R M A T I O N S E C U R I T Y

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-16
Revision 1 (2nd Draft Version 2)

A Role-Based Model for Federal Information Technology/ Cyber Security Training

Patricia Toth
Computer Security Division
Information Technology Laboratory

Penny Klein
Systegra, Inc.
Leesburg, Virginia

October 2013



U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information technology / cyber security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information technology / cyber security standards and guidelines, including minimum requirements for Federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate Federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-16
Natl. Inst. Stand. Technol. Spec. Publ. 800-16, 138 pages (October 2013)
CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Public comment period: October 30, 2013 through November 30, 2013

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: ptoth@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

Meeting security responsibilities and providing for the confidentiality, integrity, and availability of information in today's highly networked environment can be a difficult task. Each individual that owns, uses, relies on, or manages information and information systems must fully understand their specific security responsibilities. This includes ownership of the information and the role individuals have in protecting information. Information that requires protection includes information they own, information provided to them as part of their work and information they may come into contact with.

This document describes information technology / cyber security role-based training for the Federal Departments and Agencies and Organizations (Federal Organizations). Its primary focus is to provide a comprehensive, yet flexible, training methodology for the development of training courses or modules for personnel who have been identified as having significant information technology / cyber security responsibilities. This document is intended to be used by Federal information technology / cyber security training personnel and their contractors to assist in designing role-based training courses or modules for Federal Organizations personnel who have been identified as having significant responsibilities for information technology / cyber security. This publication should also be read, reviewed, or understood at a fairly high level by several audiences including the Organizational Heads through the leadership chain to the individual. Some of the titles include the IT Managers, Senior Agency Information Security Officer (SAISO), Certified Information Systems Security Officer (CISSO), Information Systems Security Officer (ISSO), Information Assurance Manager (IAM), and Program Manager (PM).

Keywords

Cyber security; information assurance; learning continuum; role-based training; security; security awareness; security controls; security literacy

DRAFT

Acknowledgements

NIST wishes to thank the members of the Federal Information Systems Security Educators' Association (FISSEA) Technical Working Group (TWG) who provided input and confirmation of various concepts that led to this version of the document.

DRAFT

Notes to Reviewers

This primary focus of this document is to provide a comprehensive, yet flexible, training methodology for the development of training courses or modules for personnel who have been identified as having significant information technology / cyber security responsibilities within Federal Organizations.

This document is intended to be used by Federal information technology / cyber security training personnel and their contractors to assist in designing role-based training courses or modules for Federal Organization personnel who have been identified as having significant responsibilities for information technology / cyber security.

Please note that several areas of the document require your suggestions and comments to complete. Appendix C, Roles is one of those areas that the authors seek your input on the approach. Additionally the authors request suggestions for figures, tables, or graphics and worked examples which may be helpful to the reader.

DRAFT

Table of Contents

Executive Summary 7

Chapter 1 - Introduction 9
- 1.1 Legislative and Policy Drivers 11
- 1.2 Relationships with Other NIST Documents 12
- 1.3 Scope 14
- 1.4 Audience 14
- 1.5 Assumptions 15
- 1.6 Document Organization 17

Chapter 2 – Perspective 19

Chapter 3 Responsibilities 22
- 3.1 Organizational Responsibilities 22
- 3.2 Agency Head 22
- 3.3 Chief Information Officer (CIO) 22
- 3.4 Senior Agency Information Security Officer (SAISO) 23
- 3.5 Managers 23
- 3.6 Training Developer / Instructional Design Specialists 24
- 3.7 Personnel with Significant Information Technology / Cyber Security Responsibilities 24
- 3.8 Users 25

Chapter 4 – Cybersecurity Learning Continuum 26
- 4.1 Security Awareness 29
- 4.2 Cybersecurity Essentials 30
- 4.3 Role-Based Security Training 31
- 4.4 Education and Experience 33
- 4.5 Role-Based Training Differs From Other Types of Training 34

Chapter 5 – Role-Based Security Training Methodology 36
- 5.1 Role-Based Security Training 36
- 5.2 Developing and Implementing Role-Based Security Training 37
- 5.2.1 Who should understand this document 37
- 5.2.2 Agency-wide Needs Assessment, Job Task Analysis and Criteria 37
- 5.2.2.3 Development Training Overview 38
- 5.2.2.4 Determination of Training Delivery 40
- 5.3. Understanding the Role-Based Training Methodology 40
- 5.3.1 Purpose of Appendices 40

Chapter 6 – Worked Example 43

Chapter 7 – Training Evaluation 45
- 7.1 Value of Evaluation in a Training Program 45
- 7.2 Purpose of Training Evaluation 45
- 7.3 Development of an Evaluation Plan 46
- 7.3.1 Behavioral Objectives 46
- 7.3.2 Types of Evaluations 47

Appendix A: Functions 51

Appendix B: Knowledge and Skills Catalog 60

Appendix C: Roles 76

Appendix D: Sample Evaluation Forms 142

Appendix E: Glossary 149

DRAFT

Executive Summary

Meeting security responsibilities and providing for the confidentiality, integrity, and availability of information in today's highly networked environment can be a difficult task. Each individual that owns, uses, relies on, or manages information and information systems must fully understand their specific security responsibilities. This includes ownership of the information and the role individuals have in protecting information. Information that requires protection includes:

- Information they own
- Information provided to them as part of their work
- Information they may come into contact with

This document describes a process to develop information technology / cyber security role-based training and its primary focus is to provide a comprehensive, yet flexible, training methodology for the development of training courses or modules for personnel who have been identified as having significant information technology / cyber security responsibilities within Federal Organizations. It should be stressed that this document is a guideline and the Federal Organizations are expected to tailor the role-based training to meet the needs of their own organization.

This document is intended to be used by Federal information technology / cyber security training personnel and their contractors to assist in designing role-based training courses or modules for Federal personnel who have been identified as having significant responsibilities for information technology / cyber security. This publication should also be read, reviewed, or understood at a fairly high level by Federal heads down through the leadership chain to the IT individual. This includes several audiences including IT Managers, Senior Agency Information Security Officer (SAISO), Certified Information Systems Security Officer (CISSO), Information Systems Security Officer (ISSO), Information Assurance Manager (IAM), and Program Manager (PM).

For the purpose of this document, these materials show how the work required to achieve a particular objective has been divided. Individuals may assume additional roles based on their individual skills, organizational policies regarding cross-training and backup, and staffing levels.

Some of the most effective current attacks on cyber networks world-wide exploit user behavior. These include phishing attacks, social engineering to obtain passwords, and introduction of malware via removable media. These threats are especially effective when directed at those with elevated network privileges and/or other elevated cyber responsibilities. Training users (privileged and unprivileged) and those with access to other pertinent information and media is a necessary deterrent to these methods. Therefore, in conjunction with Federal Information Security Management Act (FISMA) requirements, role-based training of those individuals with significant responsibility is required.

All Federal Agencies are required to have a security program implemented. There are many pieces included in the overall program. These pieces are identified in the NIST guidance, NIST 800-50, “Building an Information Technology Security Awareness and Training Program”. There are multiple initiatives and guidance to assist with building an information technology / cybersecurity program, such as the National Initiative for Cybersecurity Education (NICE). The role-based training requirement is a piece of this higher level program. Chapter 2 of this document goes into more detail on the difference between education and role-based training, and why role-based training is critical to a successful security training program.

Meeting these security responsibilities and providing for the confidentiality, integrity, and availability of

DRAFT

information in today's highly networked environment can be a challenging task. Each individual that owns, uses, relies on, or manages information and information systems must fully understand their specific security responsibilities. All managers must ensure that all users are provided awareness training, and that those identified as having significant responsibilities for information technology / cyber security are appropriately trained based on the requirements of the Federal Organization.

DRAFT

Chapter 1 - Introduction

Introduction

The Federal government must protect its information and assets. Federal laws, policies, standards, directives, regulations and guidance task individuals within Federal departments and agencies – from heads of Federal Organizations to end users, and every level in between – with a variety of security responsibilities. These responsibilities include:

- Protecting and safeguarding information,
- Identifying and categorization of systems,
- Assigning impact levels to the systems and to the information stored in and processed by those systems,
- Selecting and implementing appropriate security controls,
- Testing the effectiveness of the security controls,
- Authorizing the use of the systems,
- Authorizing access to systems,
- Maintaining an effective information technology / cyber security posture by continuous monitoring, and
- Carrying out their specific role based security-related responsibilities

Meeting these security responsibilities and providing for the confidentiality, integrity, and availability of information in today's highly networked environment can be a challenging task. Each individual that owns, uses, relies on, or manages information and information systems must fully understand their specific security responsibilities. All managers must ensure that all users are provided awareness training, and that those identified as having significant responsibilities for information technology / cyber security are appropriately trained based on the requirements of the Federal Organization. Senior Management / Leadership needs to support the role-based training. Chapter 2 of this document provides more clarification on how the role-based training plays a critical in the overall security training program.

Before proceeding further it is important to define key terms that will be used and discussed in this document. These definitions are for the purpose of this document and have been developed to provide clarity to the reader.

Awareness - the ability of the user to avoid behaviors that would compromise cybersecurity; practice good behaviors that will increase cybersecurity; and act wisely and cautiously, where judgment is needed, to increase cybersecurity.

Awareness Training - Managers must ensure that all users are provided awareness training, and that those identified as having significant responsibilities for information technology / cyber security are properly trained.

Base knowledge - the familiarity, awareness, or understanding of security gained through experience or study

Competency - the quality of being adequately qualified based on skills and knowledge

Education - knowledge or skill obtained or developed by a learning process

DRAFT

Job Function - action for which a person or thing is particularly fitted or employed

Knowledge Unit – the combination of information needed to perform a function or activity effectively and efficiently

Proficiency - the state or quality of being competent

Role - the responsibility and functions that a person is currently performing within their agency.

Training - the action provided to a user in the acquisition of knowledge, skills, and competencies in the security arena.

Roles are established by the individual Federal Organization and Agencies through position descriptions, hierarchy charts, responsibilities, etc. These Federal Organization defined roles can be matched to the generic roles used in the role-based training methodology. Roles with security related responsibilities may not be clearly stated within organizations. Everyone has a role in security even if that role does not specifically state security. For example, managers who serve as owners of systems and applications have responsibility for the overall information technology / cyber security of those systems (i.e, security of general support systems, applications, networks).

All employees must be exposed to information technology / cyber security awareness material. All users of information systems must receive awareness training, as required by the Federal Information Security Management Act. (FISMA) This awareness training helps to shape user behavior to be more secure. In today's environment, the most effective attacks on systems and networks are often via the exploitation of user behavior.

This document and NIST Special Publication 800-50, *"Building an Information Technology Security Awareness and Training Program"* describe the following key approaches of an information technology / cyber security awareness and training program that "Federal Organizations" (i.e., Federal agency / departments, Agencies or organizations) should follow to help ensure that individuals learn the appropriate information technology / cyber security-related material:

- All employees of an organization must be regularly or continually exposed to information technology / cyber security awareness. Security awareness techniques may include posters, awareness tools/trinkets, periodic e-mails, warning messages, "tips of the day" upon accessing an information system, or information technology / cyber security events.

- All users of information and information systems must attend information technology / cyber security awareness training (on-line or in-person) each year. This material should provide cyber security Essentials.

- Individuals identified by their organization as having significant responsibility for information technology / cyber security must receive formal role-based information technology / cyber security training.

NIST Special Publication 800-50, "*Building An Information Technology Security Awareness and Training Program*", provides guidance for building an effective IT security program and supports requirements specified in the FISMA and the Office of Management and Budget (OMB) Circular A-130, Appendix III. A strong IT security program cannot be put in place without significant attention given to training agency IT users on security policy, procedures, and techniques, as well as the various management, operational, and technical controls necessary and available to secure IT resources. In addition, those in the agency who manage the IT infrastructure need to have the necessary skills to carry out their assigned duties effectively. Failure to give attention to the area of security training puts an enterprise at great risk because security of agency resources is as much a human issue as it is a technology issue.

1.1.1 Who should understand this document

CIOs and other executives should refer to this document to gain a basic understanding, beyond what is mentioned in NIST SP 800-50, *"Building an Information Technology Security Awareness and Training Program*" of their organization's responsibilities regarding information technology / cyber security role-based training. An organization's CIO should understand that this document contains topics and a curriculum that can be used to develop a Cybersecurity Essentials course to meet the FISMA awareness training requirement, and a thorough training methodology that can be used to develop role-based training courses or modules for those people who have significant responsibilities for information technology / cyber security.

The senior agency information security officer (SAISO), information technology / cyber security program managers and staff, senior managers and auditors should also be familiar with the scope of this document, and should understand the applicability of the Cybersecurity Essentials course (basic security training) and of the role-based courses or modules for those who have been identified as having significant responsibilities for information technology / cyber security. The SAISOs and other information technology / cyber security practitioners should use this document to determine at which point they hand over responsibility for material development to training developers / instructional design specialists (IDS).

This document concentrates on the role-based information technology / cybersecurity training. Personnel will need to work together to meet their responsibilities which to include, but not limited to:

- Management: All levels of management will be responsible for their staff training needs; prioritize the use of training resources, identify training gaps and evaluate the training effectiveness within the work space.

- IT / Cyber Security Specialist: The IT / Cyber security specialist will be responsible for assisting, as a Subject Matter Expert (SME), in identifying training courses and training aids to meet the requirements of the roles or job functions; identify training gaps and needs within the organization's IT / Cyber security program; contributes to determining any customization that is needed and developing a compliance baseline for the organization.

- Training Professionals: This group includes human resource planners, training coordinators/curriculum developers, course developers/Instructional Development Specialists (IDS), and, of course the trainers responsible for developing, presenting and evaluating the training. This document will assist the training profession in understanding the IT security requirements and knowledge / skills required; evaluate the course quality; obtain the appropriate courses and materials; develop or customize courses/materials; and tailor their teaching approach to achieve the desired Learning Objectives.

1.1 Legislative and Policy Drivers

The Federal Information Security Management Act (FISMA), signed into law in 2002, fine-tuned long-standing information technology awareness and training requirements. FISMA clearly distinguishes between awareness efforts and training. Regarding awareness, FISMA states that an agency wide information security program includes "*security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency*." Regarding training, FISMA directs agency heads to delegate to the Chief Information Officer (CIO) the authority to ensure compliance with information security requirements, including *"training and overseeing personnel with significant responsibilities for information security . . ."* FISMA goes on to

task agency heads to "*ensure that the agency has trained personnel sufficient to assist the agency in complying with (FISMA) requirements.*" Clearly, FISMA intends organizations to identify those people who have significant responsibilities for information security and ensure they are trained to the level needed to perform their security-related tasks.

In June 2004, the Office of Personnel Management (OPM) issued a revision to the Federal personnel regulations. The changes build upon information technology awareness and training requirements contained in FISMA, and capture key concepts from NIST Special Publications 800-50 and 800-16. This regulation, 5 CFR Part 930, is entitled "*Information Security Responsibilities for Employees Who Manage or Use Information Systems*" and requires Federal organizations to provide training as set forth in NIST guidelines. Key requirements from the OPM regulation include:

- Develop an information technology awareness and training plan;
- Identify employees with significant information technology responsibilities and provide role-specific training in accordance with NIST standards and guidelines;
- Expose all users of Federal information systems to information technology awareness materials at least annually;
- Provide the following groups training that includes specific material;
  - Executives,
  - Program and functional managers,
  - CIOs, information technology program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers),
  - IT function management and operations personnel;
- Provide information technology awareness and training to all new employees before allowing them access to systems;
- Provide information technology refresher training for agency employees as frequently as determined by the agency, based on the sensitivity of the information that the employees use or process; and
- Provide training whenever there is a significant change in the agency information system environment or procedures or when an employee enters a new position that requires additional role-specific training.

Office of Management and Budget (OMB) Circular A-130, "*Management of Federal Information Resources*," Appendix III, "*Security of Federal Automated Information Resources*," also emphasizes these mandatory training requirements. Specifically, it requires that prior to being granted access to applications and systems, all individuals must receive specialized training focusing on their information security responsibilities and established system rules.

1.2 Relationships with Other NIST Documents

NIST published Special Publication 800-50, "*Building an Information Technology Security Awareness and Training Program.*" SP 800-50 was designed to be a companion document to SP 800-16, serving as a foundation document for Federal Organizations that needed to build or fine-tune an information technology and/or training program. SP 800-50 points to SP 800-16 in the section that discusses the development of information technology / cyber security training material. The two publications are complimentary – SP 800-50 works at a higher strategic level, discussing how to build information technology and training program, while this document SP 800-16, Rev. 2 is at a lower tactical level, describing an approach to information security awareness training and role-based training.

DRAFT

A companion publication to this document, NIST Special Publication 800-50, *"Building An Information Technology Security Awareness and Training Program"*, provides guidelines for building an effective information security awareness and training program and supports related requirements in FISMA, OMB Circular A-130, Appendix III, and OPM's 5CFR Part 930.

NIST SP 800-50 identifies the critical steps in the life cycle of an information security awareness and training program. Early in the life cycle of an agency's awareness and training program an agency-wide Needs Assessment should be conducted. The results of the Needs Assessment should serve as the basis of an implementation strategy, which should be developed and then approved by the organization's management. This strategic planning document identifies implementation tasks to be performed in support of established agency security training goals.

FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," introduces awareness and training as one of the eighteen areas (called "families") of minimum security requirements identified to protect the confidentiality, integrity, and availability of Federal information systems and the information processed, stored, and transmitted by those systems.

NIST Special Publication 800-53, Rev 4*"Recommended Security Controls for Federal Information Systems,"* provides more detail to the awareness and training area identified in FIPS 200. This document provides levels for each control, dependent upon the system categorization and corresponding baseline. An information system will be classified at a low, moderate or high level. As the security controls change for each level so will the intensity of the training. Four specific controls in the Awareness and Training (AT) control family include:

- AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES
  The organization develops, disseminates, and reviews/updates (organization defined) a formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entitles, and compliance; and formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

- AT-2 SECURITY AWARENESS TRAINING
  The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users; when required by information system changes; and (organization defined) thereafter.

- AT-3 ROLE-BASED SECURITY TRAINING
  The organization provides role-based security training to information system users before authorizing access to the information systems or performing assigned duties; when required by information system changes; and (organization defined) thereafter.

- AT-4 SECURITY TRAINING RECORDS
  The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for (organization defined).

Additionally, the Contingency Planning (CP) and Incident Response (IR) control families have specific controls addressing training as follows:

- CP-3 CONTINGENCY TRAINING
  The organization provides contingency training to information system users consistent with assigned roles and responsibilities before authorizing access to the information system or

DRAFT

performing assigned duties; when required by information system changes; and (organization defined) thereafter.

- IR-2 INCIDENT RESPONSE TRAINING
  The organization provides incident response training to information system users consistent with assigned roles and responsibilities before authorizing access to the information system or performing assigned duties; when required by information system changes; and (organization defined) thereafter.

NIST Special Publication 800-53A, *"Guide for Assessing the Security Controls in Federal Information Systems,"* provides guidelines for the assessment of the effectiveness of implemented awareness and training controls within an organization. Security control assessments are not about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits—rather, security controls assessments are the principal vehicle used to verify that the implementers and operators of information systems are meeting their stated security goals and objectives. Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, is written to facilitate security control assessments conducted within an effective risk management framework. The assessment results provide organizational officials with:

- Evidence about the effectiveness of security controls in organizational information systems;
- An indication of the quality of the risk management processes employed within the organization; and
- Information about the strengths and weaknesses of information systems which are supporting organizational missions and business functions in a global environment of sophisticated and changing threats.

1.3 Scope

This document describes information technology / cyber security role-based training and its primary focus is to provide a comprehensive, yet flexible, training methodology for the development of role-based training courses or modules for personnel who have been identified as having significant information technology / cyber security responsibilities within Federal Organizations. It should be noted that the trainer or training developer are not expected to be a subject matter expert (SME) in all functions but able to provide the appropriate training for a particular role. Additionally, each Federal Organization can tailor the training to fit their specific roles.

1.4 Audience

Management, from the highest to lowest levels, must understand the necessity of role-based training. Planning for the development, implementation and evaluation of role-based training within their organization is an essential function of management. All levels of management should understand how roles with security related responsibilities are identified within their organization. Management should also be aware of those roles which will require the training as well as those who will develop the training. This publication should be read, reviewed, or understood by several key audiences to include the IT senior managers and leadership, management, Senior Agency Information Security Officer (SAISO), Certified Information Systems Security Officer (CISSO), Information Systems Security Officer (ISSO), Information Assurance Manager (IAM), and Program Manager (PM) and/or individuals required to understand based on the Federal Organization's leadership structure. Target audience includes:

- Information technology / cyber security professionals that have responsibility for implementing the security role-based training portions of a Federal Organization's information technology / cyber

security awareness and training program.

- Federal information technology / cyber security training personnel and their contractors tasked with designing role-based training courses or modules for Federal Organization's personnel who have been identified as having significant responsibilities for information technology / cyber security.
- Training developer / instructional design specialist (IDS) tasked with developing and possibly delivering the awareness training and role-based training material and courses (or modules), may also use this document as guidance.

It is important to note that use of this document by the training developer and instructional designer is critical. Those who develop the training requirement and those who develop the training materials must use the same training methodology.

1.5 Assumptions

Personnel identified as having significant responsibility for information technology / cyber security should receive awareness training, Cybersecurity Essentials as discussed earlier, as well as role-based training to address their additional responsibilities. It is critical to the training developer that he/she understands the target training audience. NIST provides guidelines to assist with awareness presentations, awareness training and implementing security programs.

Personnel need to understand the basics to risk management, as defined in NIST 800-37, "*Guide for Applying the Risk Management Framework to Federal Information Systems*". The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, instructions, standards, Instructions, or regulations.

DRAFT

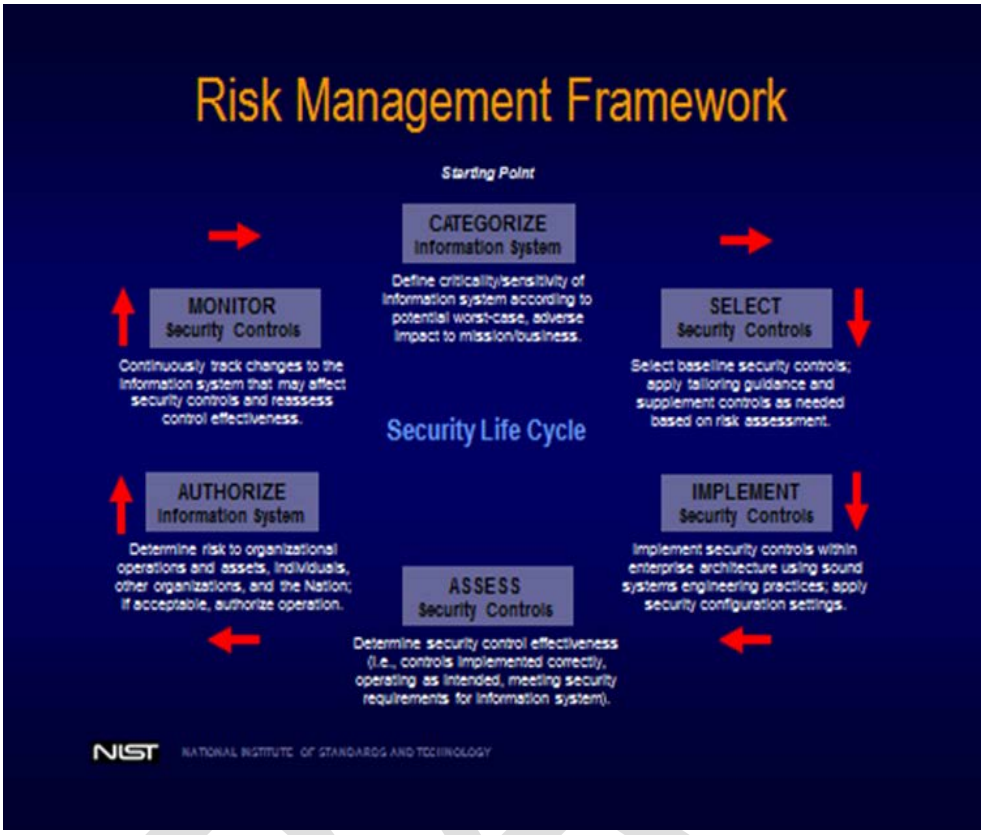


Figure 1.1, Risk Management Framework

The following activities related to managing organizational risk (also known as the Risk Management Framework – see figure 1.1) are paramount to an effective information technology / cyber security program and can be applied to both new and legacy information systems within the context of the system development life cycle and the Federal Enterprise Architecture (specific guidance can be found in the NIST SP 800-37).

- **Step 1: Categorize** the information system and the information processed, stored, and transmitted by that system based on an impact analysis
- **Step 2: Select** an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on organization assessment of risk and local conditions
- **Step 3: Implement** the security controls and document how the controls are deployed within the information system and environment of operation.
- **Step 4: Assess** the security controls using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system
- **Step 5: Authorize** information system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.
- **Step 6: Monitor** and assess selected security controls in the information system on an ongoing

basis including assessing security control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to appropriate organizational officials.

The trainees should have a base knowledge of cybersecurity essentials – familiarity, awareness, or understanding of security - from previous job experience, training, education (defined as "knowledge or skill obtained or developed by a learning process"), and their annual security awareness activity. With this annual security awareness and cybersecurity essential understanding, the following overall foundational competencies are assumed for the purpose of this document:

- Mathematics – a basic understanding of mathematics
- Organizational Awareness – a basic understanding of their organization and the threats/risks associated with it
- Quality Assurance – a program for the systematic monitoring and evaluation of the various aspects of a project to ensure that standards are being met
- Reasoning – solving a problem by considering various possible solutions
- Communications – basic writing and communication skills and an understanding of how to clearly communicate with peers
- Concepts – understands the basic intent of information assurance concepts
- Social Media – a basic understanding of the risks associated with the use of social media
- Ethics and ethical testing – conducts all evaluations and actions with approved methods and only on those systems allowed
- Teamwork -successfully work as a member of a team
- Task management – manage time according to a plan, complete tasks in a timely manner
- Use of Information Technology tools

1.6 Document Organization

This guideline is divided into four chapters and five appendices.

- Chapter 1 (Introduction) describes the legislative and policy drivers, relationships with other NIST documents, purpose and scope, audience, assumptions and outlines the organization of this document.
- Chapter 2 (Perspectives) describes the rationale, responsibilities and background needed to understand the training methodology.
- Chapter 3 (Cybersecurity Learning Continuum) describes the learning continuum (e.g., information technology / cyber security awareness, awareness training, specialized role-based training, and education), the model of the continuum and introduces the concept of role-based training.
- Chapter 4 (Role-Based Security Training Methodology) describes the implementation of role-based training, development of training, explains the purposes of the appendices and the roles and responsibilities within an organization and its people.
- Chapter 5 (Worked Example) provides a worked example of the methodology.
- Chapter 6 (Training Evaluation) describes methods of evaluating the role-based training.
- Appendix A (Functions) contains the functions within the organization and the desired Learning Objectives.

- Appendix B (Knowledge and Skills Catalog) contains appropriate knowledge and skills for each knowledge unit.
- Appendix C (Roles) contains roles and associated information
- Appendix D (Sample Evaluation Forms) contains recommendations for evaluating training effectiveness.
- Appendix E (Glossary) provides the definition for the terms used throughout the document.

DRAFT

Chapter 2 – Perspective

Role-based training is required by the Federal Information Systems Management Act (FISMA). The FISMA metrics state that "successful performance in this area would require the organization to know the total inventory of persons needing training and the content of training needed based on each person's role, the actual training provided and the user's performance result (usually test results), the difference between a and b, and have a process to address the differences by providing training or removing access rights and responsibilities." Furthermore, role-based training enhances an organization's security posture through a trained workforce and it increases the individual's readiness to respond to security incidents.

It is important to understand how the various government directives and guidelines interact with each other, and where the authority lies. FISMA is at the apex and represents the congressional mandate for role-based training. The Federal Information Processing Standards (FIPS) are written as implementers, and these include FIPS 200 and FIPS 199. Along with the FIPS, NIST 800-37, NIST 800-53, NIST 800-18 and NIST 800-50 provide additional guidance on how to meet the FISMA requirements. These various documents provide the background, authority and additional resources to assist with the implementation of role-based training

The National Initiative for Cybersecurity Education (NICE) has published a framework for the cyber workforce, including identifying various roles and functions. The NICE workforce framework should be viewed as a bridge between human resources and the cybersecurity departments. This bridge allows the Federal Government to have a view into the cyber workforce, and provides a framework on how to educate the workforce. Whereas the NICE workforce framework provides a pathway to educating the workforce, this document provides a methodology on how to train the workforce.

It is important to understand that there is a difference between Education and Training. The purpose of education is to provide learning and understanding of a subject; whereas the purpose of training is to ensure the individual can perform (doing) the functions required. For example, a pilot is *educated* on the aerodynamics of an aircraft, and *trained* on how to fly the aircraft.

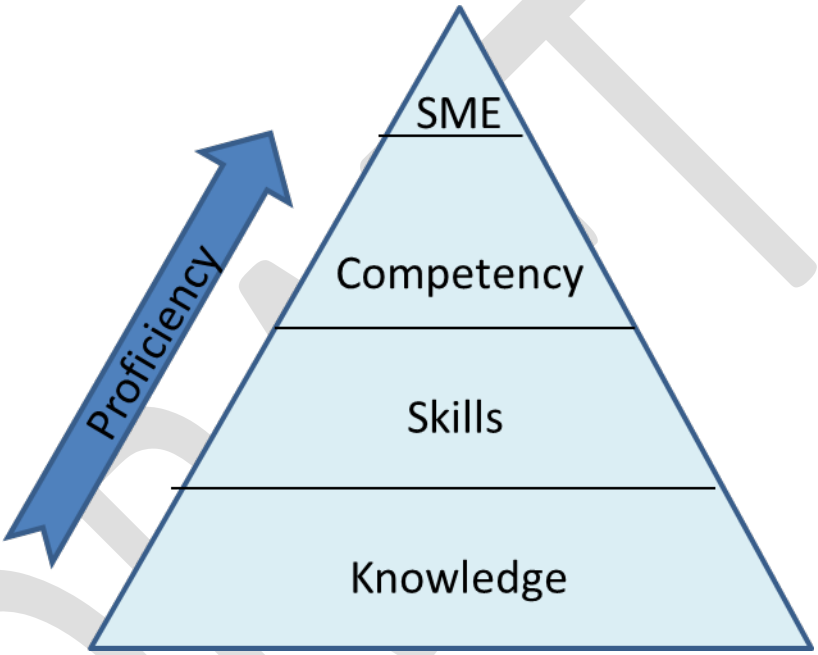
Training should be focused on providing individuals with the skills necessary to fulfill security responsibilities and functions associated with their role; roles that may or may not be IT or IT security. A role in this document is defined as the job function performed. A function is the action for which a person is specially trained. This document does not cover every role, but rather provides generic roles that can be tailored by the Federal Organization to meet their particular environment.

This document also provides guidance on the methodology to develop information technology / cyber security role-based training. This primary focus is to provide a comprehensive, yet flexible, training methodology for the development of role-based training courses or modules for personnel who have been identified as having significant information technology / cyber security responsibilities within Federal Organizations. It should be stressed that the Federal Organizations need to identify the roles within their specific organization; tailor the required or needed skills and knowledge to those roles, and ensure the training is done with any specific organizational language. It should be noted that the trainer or training developer are not expected to be a subject matter expert (SME) in all functions but able to provide the appropriate training for a particular role. Additionally, the NICE framework provides guidance in identifying roles and functions.

This document introduces the concept of Cyber Security Essentials training. There is a step (or gap) between the annual security awareness that is provided to all users, as a general introduction to good

security practices, and the role-based security training which is specific to the job functions. Cyber Security Essentials provides the understanding and/or training to address the foundational skills necessary for the role-based training to build. This training includes computer basics and literacy, and could include fundamental computer skills, basic mathematical understanding and abilities that cannot be taught, such as teamwork. The Cyber Security Essential training is further discussed in Chapter 4, the Learning Continuum.

Competencies are acquired when an individual gathers knowledge and hones skills in a certain functional area (Knowledge and Skills = Competencies). Certain roles require certain competencies, such as a security engineer requires analytical abilities to detect and identify network problems. This differs from proficiencies, which are acquired through experience and education. Proficiencies increase as the acquired competencies, associated skills and knowledge, are utilized over time.



It is critical to understand the difference between Security Awareness and Role-based Training. Security Awareness provides individuals with an awareness that there are good practices that will increase the organization's security posture, but it is not considered functional or role-based training. For example, security awareness is provided to all employees and contractors from the senior manager to the administrative assistance. The awareness agenda may identify where to find security policies, that strong passwords are required or that you must wear your identification badge above the waist.

Role-based training provides role-specific training for an individual based on their functional job and responsibilities. For example, role-based training for a network engineer will build upon the Cybersecurity Essentials and may include how to specifically set up the roles for the firewalls and the consequences if they are set up wrong. As a second example, role-based training for a senior manager may include details on the implementation of security controls, and the consequences if those controls are not implemented.

There are functions and associated roles within some Federal Organizations that are very specific. These can include functions / roles, as identified within the NICE Workforce Framework, such as Collection Operations, Cyber Operations Planning, Threat and Exploitation Analysis, All-Source Intelligence and Target Operations. Due to the sensitivity, uniqueness, and highly specialized nature of

these roles, knowledge units and supplemental guidance are not provided for these specialty areas. However, those Federal Organizations with these roles can use the current knowledge and skills to develop appropriate role-based training.

DRAFT

Chapter 3 Responsibilities

While it is important to understand the policies that require Federal Organizations to develop information technology / cyber security awareness training courses and role-based security training courses or modules, it is crucial to understand who has responsibility for security training as well as those individual who have significant security responsibilities and require the training. Personnel within Federal Organizations must understand who within their organization has the responsibility for identifying roles and developing role-based security training materials.

3.1 Organizational Responsibilities

An individual's need for information technology / cyber security training will change as their role changes. Within a particular role, over time, an individual's responsibilities may change as they assume more management, acquisition, technical, or oversight responsibility. Some roles will have more management responsibility and less technical responsibility. Some roles will have more acquisition-related responsibilities and fewer management or technically-oriented responsibilities. Some roles will have more technical responsibilities and far less management responsibilities. Others will have more oversight responsibilities.

The training methodology described in this document is flexible to account for the various responsibilities found in a role, or across many roles.

3.2 Agency Head

Agency heads must ensure that high priority is given to effective role-based training for their workforce. This includes implementation of a viable information technology / cyber security program with a strong awareness and training component. Agency heads should:

- Designate a Chief Information Officer;
- Assign responsibility for information technology / cyber security;
- Ensure that an agency-wide information technology / cyber security program is implemented;
- Ensure resources and budget are available to support the information technology / cyber security program;
- Measure the effectiveness of the information technology / cyber security program;
- Ensure that the agency has sufficiently trained and will continue to train new personnel to protect its information resources.

3.3 Chief Information Officer (CIO)

Chief Information Officers (CIOs) are tasked under FISMA to administer training and oversee personnel with significant information technology / cyber security responsibilities. CIOs should work with the Senior Agency Information technology / cyber security Officer (SAISO) to:

- Establish the overall strategy for the information technology / cyber security awareness and training program;

- Ensure that the agency head, senior managers, system and information owners, and others understand the concepts and strategy of the information technology / cyber security awareness and training program;

- Report on the progress of the program's implementation;

- Ensure that the agency's information technology / cyber security awareness and training program is funded;

- Ensure the training of agency personnel with significant information technology / cyber security responsibilities;

- Ensure that all users of information systems are sufficiently trained in their security responsibilities and other information technology / cyber Cybersecurity Essentials through awareness training; and

- Ensure that effective tracking and reporting mechanisms are in place for all facets of training.

3.4 Senior Agency Information Security Officer (SAISO)

The Senior Agency Information Security Officer (SAISO) has tactical-level responsibility for the organization's information technology / cyber security awareness and training program. In this role, the SAISO should:

- Ensure that role-based security training material is appropriately developed and delivered in a timely manner for the intended audiences;

- Ensure that role-based security training material is effectively deployed to reach the intended audiences;

- Provide an effective mechanism for feedback on role-based training security material and its presentation;

- Ensure that role-based security training material is reviewed periodically and updated when necessary; and

- Assist in establishing a tracking and reporting strategy.

3.5 Managers

Managers at all levels, from the most senior to the most junior managem, have responsibility for complying with information technology / cyber security role-based security training requirements established for their employees, users, and those who have been identified as having significant information technology / cyber security responsibilities. Managers should:

- Work with the CIO and SAISO to meet shared responsibilities and emphasize the importance of information technology / cybersecurity role-based training to the workforce;

- Serve in the role of system owner and/or information owner, where applicable;

- Consider developing individual development plans (IDPs) for those with significant information technology / cyber security responsibilities;

- Ensure that all users (including contractors) of their systems and applications are appropriately trained in how to fulfill their information technology / cyber security responsibilities prior to allowing them access;

- Ensure that users (including contractors) understand specific rules of behavior for each system and application they use; and

- Work to reduce errors and omissions by users due to lack of specialized role-based security training.

- Track all training progression and documented record training provided to employees.

3.6 Training Developer / Instructional Design Specialists

Training Developers / Instructional Design Specialists (IDSs), whether internal to an organization or external, are key players in an information technology / cyber security awareness and training program. An organization usually requires the assistance of IDSs for the development of role-based security training materials. IDSs should:

- Work with an information technology / cyber security subject matter expert when developing role-based security training material and courses to ensure that the proper material is included and is developed to the proper knowledge level for the audience; and

- Understand the role-based security training methodology in this document since it is used to develop specialized courses or modules for those individuals who have been identified as having significant responsibilities for information technology / cyber security.

3.7 Personnel with Significant Information Technology / Cyber Security Responsibilities

FISMA requires Federal Organizations to identify and train those personnel with significant information technology / cyber security responsibilities. These personnel - whether executives, information technology / cyber security program staff members, or system/network administrators - are in positions that are responsible for the security of the organization's information and information systems. Because of their positions, they can have the greatest positive or negative impact on the confidentiality, integrity, and/or availability of agency information and information systems. These personnel must:

- Attend role-based security training identified/approved by their management

- Advise their management of additional training that can help them better secure information and information systems for which they are responsible

- Understand that information technology / cyber security is an integral part of their job

DRAFT

- Understand the organizational expectations of their position
- Understand how to implement and maintain information technology / cyber security controls
- Understand how to mitigate risk to information and information systems
- Monitor the security condition of the security program, system, application, or information for which they are responsible
- Respond appropriately when security breaches are discovered
- Apply what is learned during role-based training.
- Document and record all training received.

3.8 Users

Users are the single most important group of people who can help reduce unintentional errors and related information system vulnerabilities. Users may include employees, contractors, foreign or domestic guest researchers, other agency personnel, visitors, guests, and other collaborators or associates requiring access to information and/or systems. Users must:

- Understand and comply with agency information technology / cyber security policies and procedures
- Be appropriately trained in the rules of behavior for the systems and applications to which they have access

DRAFT

Chapter 4 – Cybersecurity Learning Continuum

To successfully fulfill their roles within an organization, individuals must be given the right tools and training. The right tools and training include a combination of basic security awareness, essential skills, cooperative learning or on-the-job training, education, experience and the knowledge, skills and ability suited to the role. The Cybersecurity Learning Continuum assists in providing an approach to affording all the necessary information for individuals.

The objectives of learning are designed to permit a consistent, government-wide approach to ensure that all employees who are involved with IT systems, information technology, and cybersecurity activities - regardless of Agency, role, function, job or system – acquire the same, comprehensive understanding and training in security. The value of a consistent training program is the portability of Cybersecurity Essentials as employees change jobs and organizations.

Learning is a continuum; it starts with awareness, builds to training, and evolves into education. The Cybersecurity Learning Continuum provides context and the relationship between Security Awareness, Cybersecurity Essentials, Training and Education. The Learning Continuum demonstrates that Awareness and Cybersecurity Essentials form the fundamental baseline required for all individuals involved with the management, operation, maintenance, development or use of IT systems, information technology and cybersecurity. It also demonstrates that the training and education levels are more selective, based on a role and responsibility.

The Cybersecurity Learning Continuum as shown in figure 4-1 a progression of learning across the spectrum of roles within an organization. Security awareness training is provided to all users within an organization. Cybersecurity Essentials training is provided to all users involved with IT Systems. Role-based training is provided to users with responsibilities relative to IT Systems. Education and/or experience is gained by IT Security Specialists and Professionals. The appropriate level of Cybersecurity awareness, training and education is determined by the role within an organization. Individuals gain knowledge, and experience as they participated in role-based training with their agency.

DRAFT

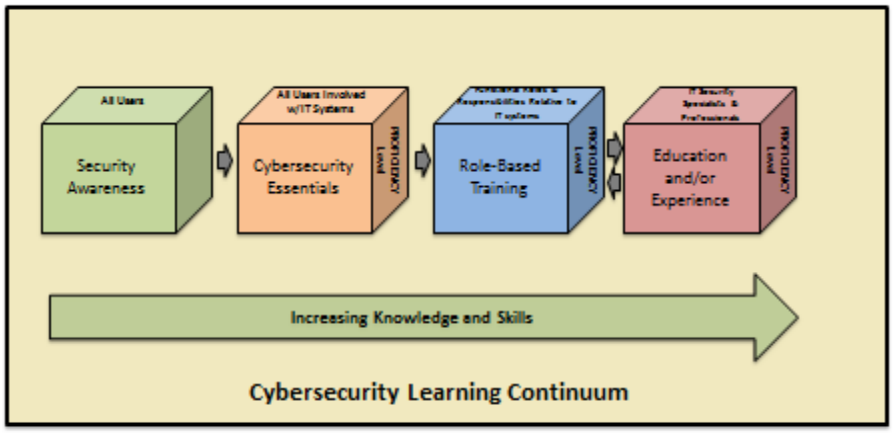


Figure 4-1: Cybersecurity Learning Continuum

The Cybersecurity Learning Continuum is designed to assist in demonstrating the level of training and awareness required for roles within an organization. This document uses generic roles and job titles that may or may not be the same as the roles or job titles used by and individual Federal Organization. The roles and titles used within this document are a sample of current jobs / roles within various Federal Organizations and organizations at the time of publication. Here is an example:

> Pearson is currently a system administrator within a Federal Organization. As an employee of a Federal Organization, Pearson must attend the annual security awareness. He is also in the Information Technology Department, so he receives additional education on cybersecurity best practices, known as cybersecurity essentials. In his role as system administrator, Pearson has significant IT responsibilities, and therefore, is required to attend role-based training.

This chapter provides a brief overview of the Cybersecurity Learning Continuum and its application within the computer security arena. The learning continuum is referenced in various NIST Special Publications such as NIST SP 800-100 and NIST SP 800-50. A model of the Cybersecurity Learning Continuum is shown in Figure 4-1. Although the curriculum provides a generic outline for material, each organization must keep in mind that it needs to relate and be tailored to their unique culture and mission requirements.

The curriculum was developed to present topics and concepts in a logical order, based on IT system planning and life cycle stages, but may be presented in any order. However, before it can be expected that an individual will be able to understand all aspects of security related to a particular role, some

exposure to basic security should have been completed. The material presented is at an introduction of the concepts and topics only, and these will be further expanded and enhanced at the role-based training level.

The model presented as Figure 4-1 is based on the premise that learning is a continuum. Learning occurs over a broad range of levels and topics. Specifically, learning in this context starts with awareness, builds to training, and evolves into education. This model provides the context for understanding and using this document, and identifying how role-based training interacts with other types of training.

The Cybersecurity Learning Continuum demonstrates that awareness and training form the baseline that is necessary for all individuals involved with the management, development, maintenance, and/or use of IT systems. It also demonstrates that role-based training and education are to be provided selectively, based on individual responsibilities and needs. Specifically, information technology / cyber security training is to be provided to individuals based on their particular roles and information technology / cyber security responsibilities, especially if they have been identified as having significant information technology / cyber security responsibilities. Information technology / cyber security-focused education is intended for designated information technology / cyber security professionals in addition to role-based training.

The Cybersecurity Learning Continuum provides the various types of learning. The type of learning that individuals need becomes more comprehensive and detailed at the top of the continuum. Thus, beginning at the bottom, all employees need to be exposed to awareness. All information system users need awareness training. Specialized training is required for individuals whose role in the organization indicates a need for special knowledge of information technology / cyber security threats, vulnerabilities, and safeguards. The "Education" layer of the model applies primarily to individuals who have made information technology / cyber security their profession.

The model illustrates the following concepts:

- "Security Awareness" is explicitly required for all employees. In today's environment this typically means all individuals within the organization.

- "Cybersecurity Essentials" is needed for those employees, including contractor employees, who are involved in any way with IT systems. Cybersecurity Essentials is the transitional stage between "Basic Awareness" and "Role-based Training." It provides the foundation for subsequent specialized or role-based training by providing a universal baseline of key security terms and concepts.

- "Role-based Security Training" becomes focused on providing the knowledge and skills specific to an individual's roles and responsibilities relative to Agency information systems. Their role within the organization is primary with IT secondary. Decision responsibilities come from the organization role, whereas the technical responsibilities are derived from the relationship with IT. At this level, training recognizes the differences between competencies among the trainees.

- "Education" focuses on developing the ability and vision to perform complex multi-disciplinary activities and the skills needed to further the information technology / cyber security profession and to keep pace with threats and technology changes. This can be accomplished with experience, cooperative training such as "on the job" training or through certification and advanced education such as undergraduate and graduate studies and degrees as accepted by the particular Federal Organization.

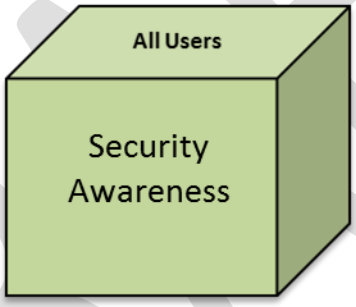
DRAFT

Learning is a continuum in terms of levels of knowledge, but the acquisition or delivery of that knowledge need not proceed sequentially. Given resource constraints, organizations have a responsibility to evaluate against the continuum both the scope of their information technology / cyber security training needs and the effectiveness of the training provided. This enables an organization to be able to allocate future training resources to derive the greatest value or return on investment.

4.1 Security Awareness

The subject of developing information technology / cyber security awareness material is discussed in NIST SP800-50, "Building an Information Technology Security Awareness and Training Program". The document is a companion publication to NIST Special Publication 800-50. The two publications are complementary – SP 800-50 works at a higher strategic level, discussing how to build an IT security awareness and training program, while SP 800-16 is at a lower tactical level, describing an approach to role-based IT security training.

The purpose of Security Awareness is to focus attention on and establish recognition of security and security issues. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.



Security awareness is a blended solution of activities that promote security, establish accountability, and inform the workforce of security news. Awareness seeks to focus an individual's attention on one issue or a set of issues. Awareness activities are intended to allow individuals to recognize information technology / cyber security concerns and respond accordingly.

In awareness activities the learner is a recipient of information. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate job performance.

Learning achieved through awareness activity alone tends to be short-term, immediate, and issue-specific. For example, if a learning objective is "to facilitate the increased use of effective password protection among employees," an awareness activity might be the use of reminder stickers for computer keyboards or global emails to all employees emphasizing the use of effective passwords.

Awareness also strives to build in an organization's information system user population foundation of information technology / cyber security terms and concepts upon which later role-based training, if required, can be based. Awareness informs users of the threats and vulnerabilities that impact their organization and personal work environments by explaining the "what" but not the "how" of security, and communicating what is and what is not allowed. Security Awareness not only communicates information technology / cyber security policies and procedures that need to be followed, but also provides the

DRAFT

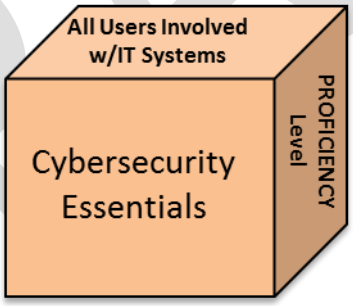
foundation for any sanctions and disciplinary actions imposed for noncompliance. Security Awareness is used to explain the rules of behavior for using an organization's information systems and information and establishes a level of expectation on the acceptable use of the information and information systems.

The fundamental value of information technology / cyber security awareness programs is that they set the stage for role-based training by bringing about a change in attitudes which should begin to change the organizational culture, which better secures the Federal organization's mission through more secure systems. The cultural change sought is the realization that information technology / cyber security is critical because a security failure has potentially adverse consequences for everyone. Information technology / cyber security is everyone's job. Detailed guidance on information technology / cyber security awareness is outside the scope of this document, but is covered in more depth in NIST SP 800-50 "Building an Information Technology Security Awareness and Training Program".

In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance

4.2 Cybersecurity Essentials

The Cybersecurity Essentials level on the Cybersecurity Learning Continuum is the transition between Security Awareness and Role-based training. This level is the foundation for further specific learning related to one's role(s) with respect to IT systems. This foundation is required before the individual can move forward in their learning. Training may be tailored to a specific organization's IT environment, security policies, and risks.



Cybersecurity Essentials, in addition to knowledge gathered via security awareness, provide a general introduction to security. FISMA requires those individuals with significant information technology / cyber security responsibilities have role-based security training. The transition from security awareness to role-based security training takes place beyond the security basics and cybersecurity essentials level.

While this document concentrates on role based training, there is an assumption that the individual has security basics knowledge. Information technology / cyber security knowledge grows commensurate with today's rapidly technology changes. Regardless of its size and growth rate, there are certain basic concepts that form the foundation of any effective IT security program and environment. These terms and concepts must be learned and applied as the individual proceeds from security awareness to training and then to education and experience.

The Cybersecurity Essentials are necessary to provide an individual with a slightly increased level security material which allows for the development or evolution of a more robust awareness program. It

may also provide the foundation for the training program.

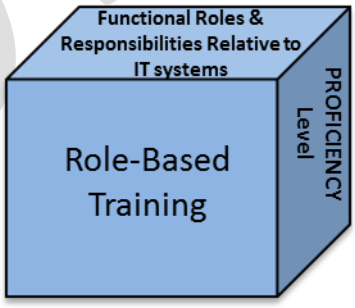
Cybersecurity Essentials must not be confused with computer literacy, as the latter refers to an individual's familiarity with a basic set of knowledge that is needed to use and maintain a computer. Cybersecurity Essentials refers to an individual's familiarity with – and ability to apply – core knowledge set which is needed to protect electronic information and systems. Cybersecurity Essentials is not geared to any specific system but rather is the foundation for further learning. All individuals who use computer technology or its output products, regardless of their specific job responsibilities, must know these essentials and be able to apply them.

The Cybersecurity Essentials level key terms, essential concepts and principles include an understanding of:

- the technical underpinnings of cybersecurity and its taxonomy, terminology and challenges
- common information and computer system security vulnerabilities
- common cyber attack mechanisms, their consequences and motivation for use
- the different types of cryptographic algorithms
- intrusion, types of intruders, techniques and motivation
- firewalls and other means of intrusion prevention
- vulnerabilities unique to virtual computing environments
- social engineering and its implications to cybersecurity
- fundamental security design principles and their role in limiting point of vulnerability

4.3 Role-Based Security Training

Roles are established by the Agency through positions, position descriptions, hierarchy charts, responsibilities, etc. These show how the work required to achieve a particular objective have been identified. Individuals may assume additional roles based on their individual skills, organization policies regarding cross-training and backup, and organizational staffing levels. Some examples of roles include: network administrator, system administrator, information assurance technician, information assurance manager, cybersecurity technician, cybersecurity manager, CISO, CIO, etc. This is just a sampling of the many roles in the information technology / cybersecurity arena and may not reflect the roles within a particular Federal Organization.



Training is more formal, is structured and has a goal of building knowledge and skills to facilitate the job performance. The purpose of awareness presentations is to focus attention on security.

The learning continuum model is role-based and defines the information technology / cyber security learning needed as a person assumes different roles within an organization and different responsibilities in

DRAFT

relation to information systems. In other words, role-based security training teaches a certain skill based on the assigned role and identifies the expected knowledge, skills and competencies from the training. Training strives to produce relevant and needed security skills and competencies. This document uses the model to identify the knowledge and skills an individual needs to perform the information technology / cyber security responsibilities specific to each of his or her roles in the organization.

Information technology / cyber security role-based training strives to produce relevant and needed security knowledge and skills within the workforce, specifically, in those individuals identified by their organization as having significant responsibilities for information technology / cyber security. Role-based security training supports competency development and helps personnel understand and learn how to better perform their specific security role, which ultimately better secures the Federal Organization's mission through more secure and protected information and systems. The most important difference between training and security awareness is that awareness is intended to make the individual recognize that there is a problem and react. Training allows that individual to react, develop and implement a proper response to vulnerabilities.

Role-based security training is required for any individual who has influence over an information system, application or network; the information; and/or organization mission. Obvious roles are the system administrator or the system developer. Less obvious roles are the program manager or procurement officer, who also needs to understand the security implications of their decision, actions or purchases. Regardless, each role has certain skills associated with that role; and that knowledge and associated skills must be taught.

Roles are not simply job titles, although a role may be associated with a job title. Roles may be job titles or functions, and are called out differently in each agency. Whatever the role is called, there are associated competencies, knowledge and skills which must be learned by the individual who occupy that role. A role-based security training curriculum may not necessarily lead to a formal degree from an institution of higher learning; however, a role-based security training course may contain much of the same material found in a course that a college or university includes in a certificate or degree program.

For illustrative purposes in this document three competency levels are described. These levels may not relate to skill or experience levels used by a particular organization.

- Competency Level I skill requirements are basic and are usually obtained during the first few years in that role. Although a person may have been working in the security arena for the last 15 years, if they move into a new role requiring additional functional skills they would need to more than Competency level I skills.

- Competency Level II skill requirements are considered intermediate, and are those skills that have obtained and honed during more years in that role.

- Competency Level III skill requirements are considered expert, and are those skills that can only be obtained after many years in the role.

Over time, individuals acquire different roles relative to their use of information and information systems and applications within their organization or as they move within various Federal Organizations. Roles can expand or change as an individual progresses through their career, either within one organization, or as they make career moves to different organizations. Sometimes they will be users of systems and applications; in other instances they may be involved in developing a new system; and in some situations they may serve on a source selection board to evaluate vendor proposals for information systems. The information technology / cyber security responsibilities that an individual has will also change over time,

and will correlate to the role that the individual has, relative to information and information systems and applications. Training must be available – whether developed within the organization, borrowed or purchased from another organization, or developed by a training company – for people in each role who have been identified as having significant information technology / cyber security responsibilities.

Here is an example of how an individual may have multiple roles during his / her career:

> Pearson has been in the IT field his entire career and has had multiple roles. He started his career as a technician on the call desk, and as such, would have been trained in that role. After a few years, he moved into a system administrator position, which required more knowledge and skills. At year 12 in his career, he changed organizations and became a team lead. This required him not only to receive training in the functional perspective of management, but also required him to learn organization specific requirements. He finally ended his career as a Senior Network Administrator. As you can see, Pearson had various roles within his career and these roles require role-based security training for those various positions.

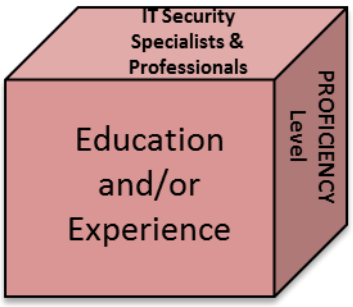
The roles listed and described in this document carry varying degrees of responsibility for information technology / cyber security, depending on what particular work an organization assigns to each role. Therefore, the person serving in one role will likely have more or less information / cybersecurity responsibility than will a person serving in another role and will need to know more about some aspects of information technology / cyber security than will a person serving in another role. For example, a CIO or SAISO/CISSO will need to know more about Federal laws and regulations and Agency policy than will a system administrator. They will need to know more about managing an information technology / cyber security program, while the system administrator will need to know far more about implementing and monitoring system-level controls, and usually far less about program management. This is why this document focuses first on roles, then on what fundamental perspective the individual has and lastly, how much experience the individual has in that particular role. All of these aspects should be considered to be included in a training course or module for each role.

There are roles within some Federal Organizations that are very specific. These can include roles, as identified within the Workforce Framework, such as Collection Operations, Cyber Operations Planning, Threat and Exploitation Analysis, All-Source Intelligence and Target Operations. Due to the sensitivity, uniqueness, and highly specialized nature of these roles, knowledge units and supplemental guidance are not provided for these specialty areas. However, those Federal Organizations with these roles can use the current knowledge and skills to develop appropriate role-based training.

The role-based security training methodology is described in Chapter 5.

4.4 Education and Experience

The Education level of the Cybersecurity Learning Continuum represents the additional option that both current and prospective information technology / cyber security professionals have to build or enhance their security-oriented knowledge and skills.



While many information technology / cyber security professionals enter the workforce with a formal education foundation, "education" as used within the Learning Continuum is meant to address the additional formal information technology / cyber security –focused education that can be obtained to augment training and experience. Education can include industry-recognized IT security certification as well as programs that are offered by higher education institutions.

To reach the advanced level of information technology / cyber security professionalization, completion of formal education in the field is often required. This professionalization integrates training, education, and experience with an assessment mechanism to validate knowledge and skills, resulting in the "certification" of a predefined level of competence. The movement toward professionalization within the information technology / cyber security field can be seen among information technology / cyber security officers, information technology / cyber security auditors, information technology contractors, and system/network administrators, and is evolving. An example of education that leads to professionalization is a degree program or certification program.

IT security education / professionalism criteria are outside the scope of this document.

4.5 Role-Based Training Differs From Other Types of Training

While the phrase "role-based training" is used extensively in this document to describe the training that should be provided to people who have significant responsibility for information technology / cyber security; role-based training may also be called "formal training," "specialized training," or "functional training" in some organizations. All of these phrases are in contrast to Cybersecurity Essentials, which is the foundation of information technology / cyber security knowledge, upon which the additional role-based training is built.

Topic-based training is training that is developed for a large group of individuals and covers a generic area; whereas role-based training allows the recipient of training to learn what he or she needs to know and be able to implement the knowledge, based on their current roles. This is perhaps the most important distinction between role-based and topic-based training. Topic based training example is training on the Time and Attendance system whereas the learning objectives for every employee is the same. While topic-based training is easier to develop because, for the most part, it can be developed once and for diverse audiences, it approaches being a one-size-fits-all solution. Unfortunately, an easy solution like this to a complex issue like information technology / cyber security training can in itself be considered as a vulnerability as dangerous as a poorly configured operating system or firewall. Recipients of topic-based training, for the most part, must interpret what they see and hear during a training session, determining what it is that they need to learn and be able to do and what does not apply to them, based on their role.

Typically, material included in a topic-based training course is meant to be consumed by people who fill a number of different roles. For example, "generalists" – those attendees in many management-oriented

roles – who need to understand some information about many different topics are likely going to be overloaded with details about topics about which they need to know little. Conversely, "specialists" – those attendees in many technical roles – who need to be exposed to relatively fewer topics, but must understand these topics in far greater depth, are more than likely going to be disappointed when those topics are not adequately addressed, therefore, the training will not meet their needs. Therefore, role-based training - which tailors the training to the role, functional perspective and experience – is required within the security arena.

Throughout their career, individuals acquire different roles relative to the use of IT systems and information within an organization, or as they transition to other organizations. In these various roles, they may be an user, administrator, manager or developer. They could even have the roles of a source-selection team for a new IT system, or developing the budget to maintain the IT system and as such, its security baseline. Therefore, the needs for training change as the roles change. To address this change, the role-based training level has been segmented into categories of generic areas:

- Manage – the individual's job functions encompass overseeing a program or technical aspect of a security program; overseeing the lifecycle of a computer system, network or application; or have responsibilities for the training of staff

- Design – the individual's job functions encompass scoping a program or developing procedures, process and architectures; or design of a computer system, network or application.

- Implement – the individual's functions encompass putting programs, processes, polices into place; or operation / maintenance of a computer system, network or application.

- Evaluate – the individual's functions encompass assessing the effectiveness of any of the above actions.

These categories will be further explained in Chapter 5 of this document.

Within each of these areas, the trainer should tailor the knowledge and skills to address the individual's role and competency. That is, are they relatively new to the area – such as becoming a team lead from an administrator position? Or are they very experienced from having been in that role for years?

DRAFT

Chapter 5 – Role-Based Security Training Methodology

5.1 Role-Based Security Training

As previously discussed, this role-based security training level includes the security-related experience as well as the specific area the individual occupies. Functional perspectives are also helpful to identify and scope requirements for each role and enhance the training development and outcomes. For the purposes role-based training, the following specific functions are generically defined as follows:

- **Manage:** Functions that encompass overseeing a program or technical aspect of a security program at a high level, and ensuring currency with changing risk and threat environments; including the management of any program, persons, or operations.

- **Design:** Functions that encompass scoping a program or developing procedures, processes, and architectures that guide work execution at the program and/or system level; as well as the secure development of systems, networks or applications.

- **Implement:** Functions that encompass putting programs, processes, or policies into action within an organization; including operation and maintenance of systems, networks or applications.

- **Evaluate:** Functions that encompass assessing the effectiveness of a program, policy, process, or security service in achieving its objectives; including the evaluation of the security state of a system, network or application.

In addition to the functional perspectives, the amount of experience the individual possesses needs to be considered when providing role-based security training. Experience / proficiency or competency levels are defined by each Agency.

All of these areas are used to tailor the training to the specific role.

To further explain the importance of functional perspective, we will revisit "Pearson" as an example to show how the area and competency level works.

> Pearson has been in the IT field his entire career. He started his career as a technician on the call desk, and as such, would have been trained in that role. For this role, the training module would have to cover those requirements in "implement" at Competency Level I. After a few years, he moved into a system administrator position, which required more knowledge and skills. His training requirements in this position were functionally aligned with either "implement" or "evaluate" and his competency was at Competency Level 1I since some of the experience he acquired as a technician can be applied to his system administrator position. At year 12 in his career, he changed organizations and became a team lead. He was then trained for his functional role to "manage" and returned to a Competency Level I since this is a new area for him. He finally ended his career as a Senior Network Administrator - we will assume that Pearson had at least 10 years in this role so he would be trained to "implement" and is now at Competency Level III.

DRAFT

5.2 Developing and Implementing Role-Based Security Training

5.2.1 *Who should understand this document*

CIOs and other executives should refer to this document to gain a basic understanding, beyond what is mentioned in NIST SP 800-50, *"Building an Information Technology Security Awareness and Training Program*" of their organization's responsibilities regarding information technology / cyber security role-based training. An organization's CIO should understand that this document contains topics and a curriculum that can be used to develop a Cybersecurity Essentials course to meet the FISMA awareness training requirement, and a thorough training methodology that can be used to develop role-based training courses or modules for those people who have significant responsibilities for information technology / cyber security.

The Senior Agency Information Security Officer (SAISO), information technology / cyber security program managers and staff, and auditors should also be familiar with the scope of this document, and should understand the applicability of Cybersecurity Essentials and role-based courses or modules for those who have been identified as having significant responsibilities for information technology / cyber security. The SAISOs and other information technology / cyber security practitioners should use this document to determine at which point they hand over responsibility for material development to training developers / instructional design specialists (IDS).

This document concentrates on the role-based information technology / cybersecurity training. Personnel will need to work together to meet their responsibilities which to include, but not limited to:

- Management: All levels of management will be responsible for their staff training needs; prioritize the use of training resources, identify training gaps and evaluate the training effectiveness.

- IT / Cyber Security Specialist: The IT / Cyber security specialist will be responsible for assisting in the identification of (1) the requirements of the roles or job functions; (2) training gaps and needs within the organization's IT / Cyber security program; (3) customization that is needed and (4) a compliance baseline for the organization.

- Training Professionals: This group includes human resource planners, training coordinators/curriculum developers, course developers/Instructional Development Specialists (IDS), and, of course the trainers responsible for developing, presenting and evaluating the training. This document will assist the training profession in understanding the IT security knowledge / skills required; evaluate the course quality; obtain the appropriate courses and materials; develop or customize courses/materials; and tailor their teaching approach to achieve the desired Learning Objectives.

The training methodology described in this chapter focuses on providing the training developer / IDS or course developer, with the tools to build a course or module based on the information technology / cyber security role of the intended audience.

5.2.2 Agency-wide Needs Assessment, Job Task Analysis and Criteria

Before any training should be created, a Federal Organization might want to know their training requirements, tasks and criteria to be met. Having this fundamental information ensures the training is

targeted to meet the Federal Organization's mission and information technology / cybersecurity needs, and addresses the variety of roles within the Federal Organization. It is suggested the Federal Organization role-based security training be based on the results of a Federal Organization-wide Needs Assessments, which should identify any role-based training requirements. This chapter describes, at a high level, the steps to develop the role-based security training.

5.2.2.1 Agency-wide Needs Assessment

An Agency-wide Needs Assessment is helpful in beginning to establish and depict the training requirement for an organization. Conducting the Needs Assessment will assist in identifying any gaps in the organization's current role-based training program, as well as any gaps in the current role-based security training. Management must identify the skills required to perform the functions they assigned to specific Agency roles. The role requirements are then analyzed to identify the learning required to acquire those skills and how it is expected to be acquired (formal training, OJT, etc.). The focus of this document is to develop the role-based security training, not to conduct the Needs Assessment. The method of conducting a Needs Assessment is covered in other NIST documents.

Another important result of the Needs Assessment is the related information technology / cyber security role-based training program requirements. For example, if role-based security training material will be presented utilizing computer-based training (CBT) technology, a technical assessment should be conducted on the organization's processing platform (e.g., local area network, workstations, video cards, speakers) to determine if the existing environment will support the new or expanded training program.

The Needs Assessment will identify the relationship between identified role-based security training requirements and an organization's current efforts. The Needs Assessment helps identify these additional needs – the gap between what is currently being done and what is required. This should be completed prior to the development of training modules.

5.2.2.2 Job Task Analysis and Criteria

Although various organizations may use the same role name to describe or label people who do similar work, the actual knowledge and skills needed by incumbents in same-titled positions may vary from organization to organization, and even within the same Agency. A job task analysis that focuses on work currently being accomplished by people in the same role, or perhaps more accurately, doing what is perceived to be the same work, will highlight what training is needed, or how existing training courses or modules should be modified to meet employee needs.

There may be instances in which some people in a role, but not all, are identified as having significant information technology / cyber security responsibilities. Depending on the criteria that an organization uses to make this determination – e.g., impact level of associated information, information system, or application; position sensitivity identified in position descriptions; significant information technology / cyber security responsibilities identified in performance plans; specific personnel named in system security plans – some members of a role may be selected for training, while others who do not meet the organization's criteria may not be required to attend the training. While these personnel may not be required to attend the role-based security training designed for those with significant information technology / cyber security responsibilities, their supervisors will likely insist that they receive some training - role-based or topic-based – even the same training as others in the same role.

5.2.2.3 Development Training Overview

After identifying the roles that require training, or any gaps in the current training, the development of

the training modules can be completed. The appendices in this document can assist with the ensuring that the training meets the requirements of the role.

"Scoping guidance" was first used in NIST SP 800-53. Here, in the context of role-based security training, "scoping guidance" is used to describe the flexibility an organization has to build, or have built, information technology / cyber security courses or modules, using the results of Needs Assessments, job task analyses, and the training methodology described in this chapter. It is highly suggested that the organization scope the development of the training to meet the roles of their particular organization, and use the terminology that is understood by their employees.

The identification of a role or roles in need of training would be accomplished by: 1) a Needs Assessment, 2) an inspector's review, or 3) the person or people in the organization tasked with identifying those with significant information technology / cyber security responsibilities. These processes can also identify whether training is to be developed where none exists for a role or roles, or if existing training needs to be updated or modified. Regardless of how roles are identified for information technology / cyber security training within an organization, supervisors remain the best barometer of individual training needs. Using position descriptions, performance plans, and individual development plans, supervisors - with input from their staff - can identify training needs. By coordinating with the organization's information technology / cyber security training function, supervisors can determine if the needed training is available in-house, or must be sought elsewhere.

Various methods to develop training are available to the Training Developer / IDS. The developer should ensure that the complexity of the training is commensurate with the role and the needs of the person or people who will undergo the learning effort. Material should be developed based on two important criteria: 1) the role, and 2) knowledge and skills identified for that position.

When developing the training, keep in mind these key steps:

- Write an explanation of expected core skills to be learned. This is an overview of what class participants can expect to learn after progressing through the training materials.
- Establish learning objectives in accordance with the organizational mission.
- Dedicate a separate section to each learning objective.
- Create individual lessons for each of the learning objectives.
- Integrate visual elements; Use graphics, videos, tables and other visual tools to reinforce important concepts.

Training can be developed via various methods, which could include but are certainly not limited to, ADDIE, Dick and Carey Systems Approach, Instructional Development Learning System (IDLS), and Kemp. In addition to various development methodologies, there are various training methodologies. These could include, but not limited to, computer based training, classroom training, on-line courses and on-the-job training.

Training must be developed and provided if no such training exists for a role, if the organization has identified that role as having significant information technology / cyber security responsibilities.

The list of roles is provided in Appendix B can be used by a course developer / IDS. Appendix A provides functions that may require role-based training. Specifically, Appendix A provides:

- Function Areas
- Roles Areas - these roles are guidance and may exist under different names within a particular Agency
- Definitions of the functions

DRAFT

- Learning Objectives of the training

Appendix B provides the Knowledge and Skills that are required in each competency.

Appendix C provides a more comprehensive view into the roles. This appendix expands on the functions previously identified. Specifically, Appendix C provides:

- Function Area - which corresponds with Appendix A: Functions
- Role Area - - these roles are guidance and may exist under different names within a particular Agency
- Role(s) - a general list and can be tailored to match the specific roles within the agency;
- Responsibility of the role area
- Knowledge Unit - identifies the competencies associated with the role
- Knowledge and Skills Table – correspondents to the knowledge unit

5.2.2.4 Determination of Training Delivery

Types and methods of training need to be determined prior to the development of the training. Training methods can be self-directed, information, formal, etc. One Agency may choose to use computer-based training (CBT) while another may use classroom presentations, seminars or some other type of formal training.



5.3. Understanding the Role-Based Training Methodology

5.3.1 Purpose of Appendices

Overall, Appendices A through D provide the essential elements for developing role based training. They provide guidance and information to determine functions, outline role skills and knowledge, identifies knowledge units, and provides a method for evaluating training.

DRAFT

For the purpose of this document Appendix A and Appendix B use the following terms:

- Competency - the quality of being adequately or well qualified physically and intellectually.
- Knowledge Unit – the combination of information needed to perform a function or activity effectively and efficiently

5.3.1.1 Appendix A: Functions

Appendix A is designed to assist in determining which functions and roles should be identified as candidates for role-based security training. Additionally, the outcomes for these functions are outlined.

The format for this Appendix is as follows:

- **Function Area:** Identifies a security function area.
- **Roles Areas:** Identifies various roles that are covered by the function. These roles are guidelines and may exist under different names within a particular Agency.
- **Definition:** Provides a definition of the function.
- **Learning Objectives(s):** Identifies the various outcomes that the training module should strive to meet for each of the functions and their associated roles.

5.3.1.2 Appendix B: Knowledge and Skill Catalog

This appendix contains each knowledge unit. Within each knowledge unit are the associated knowledge and skills. The knowledge and skills are specific and the training developer must ensure that these are covered in their training modules.

5.3.1.3 Appendix C: Roles

Appendix C is designed to assist in determining which competency/knowledge unit and associated Knowledge and Skills are required by a particular role. The generic roles and job titles used within this Appendix may or may not be the same as the roles or job titles used by and individual Agency or organization. The ones used within this Appendix are a sample of current jobs / roles within various Federal Organizations and organizations at the time of publication. Using the competencies and functions, each of these samples can be tailored to meet the roles within a specific Agency.

All roles should have training on the Overall Knowledge and Skills as described within Appendix C, Knowledge Units, Knowledge and Skills Catalog. These are the fundamental basis of knowledge/skills required for all jobs and roles.

The format is as follows:

- **Function Area**: This area corresponds with *Appendix A: Function Area*. Appendix A provides a general description of the area and the Learning Objectives for those functions. The roles described within this appendix are within a function.
- **Role Area**: This describes the overall role.

DRAFT

- **Roles**: Identifies various roles that are covered by the function. These roles are guidelines and may exist under different names within a particular Agency. Provided to assist in determining who should receive this role-based training.
- **Responsibility**: Defines the activities, tasks and / or responsibilities of that particular role.
- **Knowledge Unit**: Identifies the competencies associated with the role. The entire listing of the knowledge units and their associated knowledge and skills are located in *Appendix B: Knowledge and Skills Catalog*.
- **Corresponding Knowledge and Skills Table**: This table provides a breakdown of the specific knowledge unit, the corresponding knowledge and skills to each competency. Each role has various knowledge units associated with it. There are 4 differing areas that correspond with the job title to allow for further tailoring of role training to better match with the job function. These areas are defined as follows:
    - **Manage** – those knowledge and skills particular to those employees who are responsible for management (e.g., managers, team leads, project managers)
    - **Design** – those knowledge and skills particular to those employees who are responsible for design activities (e.g., system developers, engineers)
    - **Implement** – those knowledge and skills particular to those employees who execute implementation (e.g., system administrators, network administrators)
    - **Evaluate** – those knowledge and skills particular to evaluation activities (e.g., testers, security analysts)

5.3.1.4 Appendix D: Sample Evaluation Forms

The forms that will assist in the evaluation of the training are located within this appendix.

Although this document includes a number of role-based matrices in Appendices, this by no means suggests that any organization should have to build training courses or modules for each role. The Appendices should be viewed as a catalog of role-specific matrices, some of which will be used to build courses or modules. Organizations should have identified those personnel or roles needing role-based training, based on their having significant information technology / cyber security responsibilities, before using this document.

DRAFT

Chapter 6 – Worked Example

This chapter provides a worked example of how to use this methodology. First is the layout of the steps, which is followed by an example.

The first step in developing role-based security training is conducting the Agency-wide Needs Assessment. This action will identify any gaps in the current training program, and/or identify those roles which require training. The guidance for conducting a Needs Assessment is outside the scope of this document, but can be found in NIST 800-50.

Once this activity is completed and the role-based training area(s) identified, the second step is functions identification. Appendix A, or Functions appendix, should be seen as a catalog, whereby an organization would begin the process to develop training material for a course or module. It is important to understand that just because a function or role is listed within the appendices; it does not mean that a training course or module must be built for that role. The Needs Assessment will identify those required modules. Training must be identified, developed and provided if no such training exists for a role which the organization has identified as having significant information technology / cyber security responsibilities. Existing training must be enhanced or a similar course identified and provided if evaluation feedback, Needs Assessment and/or job task analysis indicates that current training is not meeting the information technology / cyber security needs of the intended audience.

After the functions are identified, the third step is to annotate the associated training outcomes and learning objectives. This provides the target for the training developer / IDS. Using the identified function, Appendix B will provide some associated role areas and roles and help shape the learning objectives. These provide the training developer / IDS with the ability to tailor to match the roles and terminology that the organization utilizes. Using the appropriate role, the corresponding knowledge and skills can be identified. Additionally, these can be further refined by the role's functional perspective, whether that be the functional perspective of manage, design, develop or evaluate. Learning objectives should be observable and measurable and ensure they meet the organization mission.

In the fourth and final step the training developer can tailor the training module to the appropriate level of expertise for the audience.

Role-based security training can now be developed. An example of how this would work follows.

The first activity is to conduct the Agency-wide Needs Assessment. This action will identify those role areas that require training. For this example, we will assume that the organization's contracting office has not been including security requirements in the awarded contracts. In this example, the Needs Assessment determined that an individual, has not been trained in any security areas which is identified as a training gap. The individual is a Contracts Officer, with 10 years of contracting experience and two years ago moved into IT / Cyber contracts.

The second activity is to identity the function with which the training gap is associated, as defined in Appendix A. For this example, the function area is Oversight, Management and Development and the role area is Procurement. The outcomes for this training are also listed in Appendix A and as the training is developed, Learning Objectives(s) should be in the forefront, (e.g., Provides contractual, procurement and/or acquisition support for IA purchases). Additionally, the actual job title can be traced to a Role / Function, (e.g., Procurement).

DRAFT

Once the function and role area has been identified, then Appendix B should be reviewed. The roles listed in Appendix B can be tailored to match those roles/job titles of the organization. At this point, the role tasks that the employee executes determine the level to which he / she needs to be trained. In our example, the Contracting Officer has 10 years of experience in contracting, but has only within the last 2 years moved into IT / Cyber contracting. The employee is well versed and understands contracting requirements, but needs to be trained specifically on the security requirements that are associated with IT / Cyber contracting. Therefore, with only 2 years in IT / Cyber contracting, the employee is at a Competency level I. This competency level determines the Knowledge Units that will be used to develop the training module.

The Knowledge Unit is based on the competencies identified for that role and the knowledge and skills required to successfully execute the activities associated with the role. Each competency level will determine how far in depth is associated with role.

In addition to the Competency levels, the functional perspective of the role must be considered. There are four (4) functional perspectives: Manage, Design, Implement and Evaluate. For this example, the role requiring training is the Contracting Officer(s) who are awarding the contracts. We will assume that the contracts have been written and this role is reviewing to ensure that the contracts are ready for award. Therefore, we will use those knowledge and skills identified in the "Manage" column in Appendix B Module for Roles.

In the Manage column are the following competency, knowledge and skills:

- Knowledge Unit – ***Procurement***
  - Knowledge and Skills:
    - *PROC-6; PROC-7; PROC-8; PROC-9; PROC-11; PROC-12*

- Knowledge Unit – ***Management***
  - Knowledge and Skills:
    - *PM-1; PM-2; PM-3; PM-4; PM-8; PM-10; PM-12; PM-14; PM-16; PM-22; PM-23; PM-25; PM-32; PM-33*

- Knowledge Unit – ***Compliance***
  - Knowledge and Skills:
    - *COMP-1; COMP-3; COMP-4; COMP-5; COMP-7*

Next, we will go to Appendix C. This appendix will specifically state what knowledge or skill the role contains. Using the above example, *PROC-6* means that the training module should provide the employee with knowledge about how to execute secure acquisitions.

The employee is trained specifically to his/her role as well as the corresponding responsibilities of that role. As the training module is developed, these knowledge and skills must be included with the outcome as defined for the function.

Once the training is complete, then an evaluation should be conducted. The next chapter provides guidance on how to successfully evaluate the training. Appendix D provides samples forms to assist with evaluating the training. Any areas of training that were confusing or did not provide the desired outcome can be identified through the evaluation process and should be improved prior to the next training session.

DRAFT

Chapter 7 – Training Evaluation

7.1 Value of Evaluation in a Training Program

Evaluating training effectiveness is a vital step to ensure that the training delivered is meaningful. Training is meaningful *only* when it meets the needs of both the student (employee) and the organization (employer). If training content is incorrect, outdated, or inappropriate for the audience, the training will not meet student or organizational needs. If the delivery vehicle (e.g., classroom, computer-based training, web-based training) is inappropriate, either in relation to the simplicity/complexity of the content or to the type of audience, the training will not meet the needs of the student and the organization. Spending time and resources on training that does not achieve desired effects can reinforce, rather than dispel, the perception of security as an obstacle to productivity. Further, it can require the expenditure of far more resources in data or system recovery after a security incident occurs than would have been spent in prevention activities such as training.

All meaningless training is expensive, even where the direct cost outlay, or cost-per-student, maybe low. Federal Organizations cannot afford to waste limited resources on ineffective training, consequently, evaluation of training effectiveness should become an integral component of an agency's information technology / cyber security training program. A robust training evaluation effort may be the second most effective vehicle for garnering management support for information technology / cyber security with the first is the occurrence of a serious security incident.

7.2 Purpose of Training Evaluation

Meaningfulness of training, or its effectiveness, requires measurement. Evaluating training effectiveness has four distinct but interrelated purposes—to measure:

- The extent to which conditions were right for learning and the learner's subjective satisfaction;
- What a given student has learned from a specific course or training event, (i.e., learning objectives and effectiveness);
- A pattern of student behavior or outcomes following a specific course or training event; (i.e., teaching effectiveness); and
- The value of the specific class or training event compared to other options in the context of an agency's overall information technology / cyber security training program; (i.e., program effectiveness).

An evaluation process should produce four types of measurement, each related to one of evaluation's four purposes, as appropriate for three types of users of evaluation data:

1. Evaluations should assist the employees themselves in assessing their subsequent on-the-job performance.
2. Evaluations should assist the employees' supervisors in assessing individual students' subsequent on-the-job performance.
3. Evaluations should produce trend data to assist trainers in improving both learning and teaching.
4. Evaluations should produce return-on-investment (ROI) statistics to enable responsible officials to allocate limit resources in a thoughtful, strategic manner among the spectrum of security awareness, cybersecurity essentials, role-based security training, and education options

DRAFT

for optimal results among the workforce as a whole.

7.3 Development of an Evaluation Plan

It is often difficult to get good information for each of evaluation's four purposes, as described above, and it is impossible to do so without planning for evaluation. To evaluate student learning, it is first necessary to have written learning objectives, stated in an observable, measurable way as Learning Objectives or behavioral objectives. To evaluate teaching, it is necessary to plan for the collection of trend data, evaluation, and extrapolation. To evaluate return on investment (ROI), mission-related goals must be explicitly identified to which the learning objectives are related. The remainder of this section provides guidance in the development of an Evaluation Plan.

7.3.1 Behavioral Objectives

The major components of behavioral objectives are:

- Conditions of Activity – written description of the existing conditions and the learning activity
- Activity to be Performed – how the activity will be performed in order to allow the student to learn
- Level of Success – how has the student's performance on the job changed as a result of the information learned

There are several schools of behavioral objectives among educational theorists; however, most agree with the three components, described below.

7.3.1.1 Conditions of Activity

This is a written description of existing conditions prior to, and in preparation for, the learning activity. Certain conditions must be present to forecast training effectiveness. Does the student need a checklist, a set of items to manipulate, or an outline of the information? Does the instructor need audiovisual equipment, handouts, or a classroom with furniture set up in a specific format? Conditions of the learning activity, including Computer-Based Training (CBT), not just platform training, must be specific and comprehensive.

7.3.1.2 Activity to be Performed

The evaluation plan must state the activity to be performed in a manner permitting the evaluator to actually observe the behavior that the student is to learn—which is observable in class (teacher as evaluator) or back on the job (supervisor as evaluator). It is difficult, if not impossible, to measure the process of a student's changing attitude or thinking through a task or problem. The evaluator, however, can measure a written exercise, a skill demonstration, a verbal or written pronouncement, or any combination of these outwardly demonstrable activities. He/she cannot take the student's word for the learned skill, or rely on the simple fact that the student was present and exposed to the skill or information being taught. Rather, the evaluator must observe the skill being performed or the information being applied. With CBT, evaluation measurement can be programmed to occur at the instructional block level, with subsequent blocks adjusted based on a student's response. Platform training differs from Computer Based Training (CBT) since platform training has an instructor in the classroom. With platform training, adjustments can be made in real time by the instructor based on the nature of student questions during the course. Adjustments can also be made between courses in a student's training sequence.

7.3.1.3 Levels of Success

Measures of success should be derived from the individual's normal work products rather than from

DRAFT

classroom testing. This directly ties the individual's performance to its impact on the organization's mission. Written behavioral objectives for a learning activity must include a stated level of success. For quantitative skills, must the learner perform successfully every time, or 10 out of 100 times, or 5 out of 10 times in terms of performance requirements or consequences? Risk management requirements should be used to establish the criticality of quantitative skills. For qualitative skills, what distinguishes satisfactory performance from failure, or outstanding performance from satisfactory? Measurements of qualitative skills might include the amount of re-work required, customer satisfaction, or peer recognition of the employee as a source of information technology / cyber security information.

The nature and purpose of the training activity, and whether it is at a beginning, intermediate, or advanced level, will influence the setting of success measures. If success levels are not documented, an individual student's achievement of the behavioral objectives of the learning activity can not be evaluated, nor can the learning activity itself be evaluated within an organization's overall training program.

In addition to the written objectives suggested above, the evaluation plan should show how the collected data is to be used to support the cost and effort of the data collection. This can be related to types of evaluations, presented next.

7.3.2 Types of Evaluations

One type of evaluation is to conduct an exercise that allows training participants to test/validate the knowledge of learned behavior following courses. Through this exercise, the trainer can identify areas that may need improvement.

For all types of evaluation, a critical step is to ensure the feedback is considered in the continuous training process. Regardless of the type of evaluation that is implemented, the feedback must be looped back into the training material. For example, if a student states that chapter 2 was vague, that chapter should be updated for clarity prior to the next training session.

7.3.2.1 Student Satisfaction

A common term for this type of evaluation is the 'Smiley Face' evaluation. Likert Scale-type forms ask the student to check a range of options from poor to excellent (or *vice versa*) to indicate how he/she felt about the class, the computer-based courseware, or whatever the learning activity was. The response data is an indicator of how the learning activity is received by the student. The responses also reveal if the conditions for learning were correct. Some of the questions in this level of evaluation ask about the student's satisfaction with the training facility and instructor (if classroom training), the manner of presentation (of the content), and whether or not course objectives were met in relation to the student's expectations. Although this type of evaluation does not provide in-depth data, it does provide rapid feedback from the learner's perspective. Measurement of training effectiveness depends on an understanding of the background and skill level of the training audience.

7.3.2.2 Learning and Teaching Effectiveness

This level of evaluation measures how much information or skill was transmitted from the training activity to the learner or student. The evaluation should be in various formats relative to the level of training. For example, at an intermediate or advanced role-based training level, participants should be given some sort of performance test, such as a case study to solve. The evaluation format must relate back to the behavioral objectives of the learning activity, which, in turn, drives the content being presented. The evaluation also provides instant feedback, and it assesses how much the student remembered or demonstrated by skill performance by the end of the program, not how he/she felt about

it. Evaluation can be built into each block of instruction and does not need to wait until the end of a course.

An evaluation measures success in transference of information and skills to the student. It enables the evaluator to determine if a given student may need to repeat the course, or perhaps attend a different type of learning activity presenting the same material in a different format (if available). The evaluator should be able to see if a pattern of transference problems emerges, and determine whether or not the course itself may need to be reconfigured or perhaps dropped from an organization's training program.

Behavior objective testing is possibly the most difficult measurement area to address. It is relatively easy to test the knowledge level of the attendees after completing a course or block of instruction, but it is not easy to determine when that learning took place. An attendee may have had knowledge of the subject area before receiving the instruction, so the course may have had little or no impact. Thus, information collected solely at the conclusion of a course/instructional block must be examined relative to the attendee's background and education.

To better determine the learning impact of a specific course or instructional block, one approach is to use pre/post-testing, in which a test or testing is performed at the outset of the course. The results are then compared to testing conducted at the conclusion of instruction.

Testing of an attendee's knowledge of a particular subject area by including questions or tasks where there is a single right answer or approach, is appropriate for almost all testing situations, especially at the beginning and intermediate levels. Questions regarding selection of the best answer among possible options should be reserved for those training environments where there is opportunity for analysis regarding why a particular answer is better than other answers.

7.3.2.3 Student Performance Effectiveness

This evaluation is the first level which asks for more than student input. At this level, the evaluator, through a structured questionnaire usually administered 30 to 60 days following the training activity, asks the supervisor about the performance of the employee(s) relative to the behavioral objectives of the course. This is a before and after job skills comparison. In some cases this information is difficult to obtain, especially when employees' roles and seniority levels permit them considerable autonomy, without direct supervision. When supervisors observe only the final output of employee actions, developing a valid questionnaire can present a particular challenge. When accomplished successfully, a Level 3 evaluation should begin to show the extent to which the learning activity benefits the organization as well as the employee. The learner's supervisor may determine whether the learner used the knowledge obtained in the course to accomplish job tasks, or whether the learner's performance improved since taking the course.

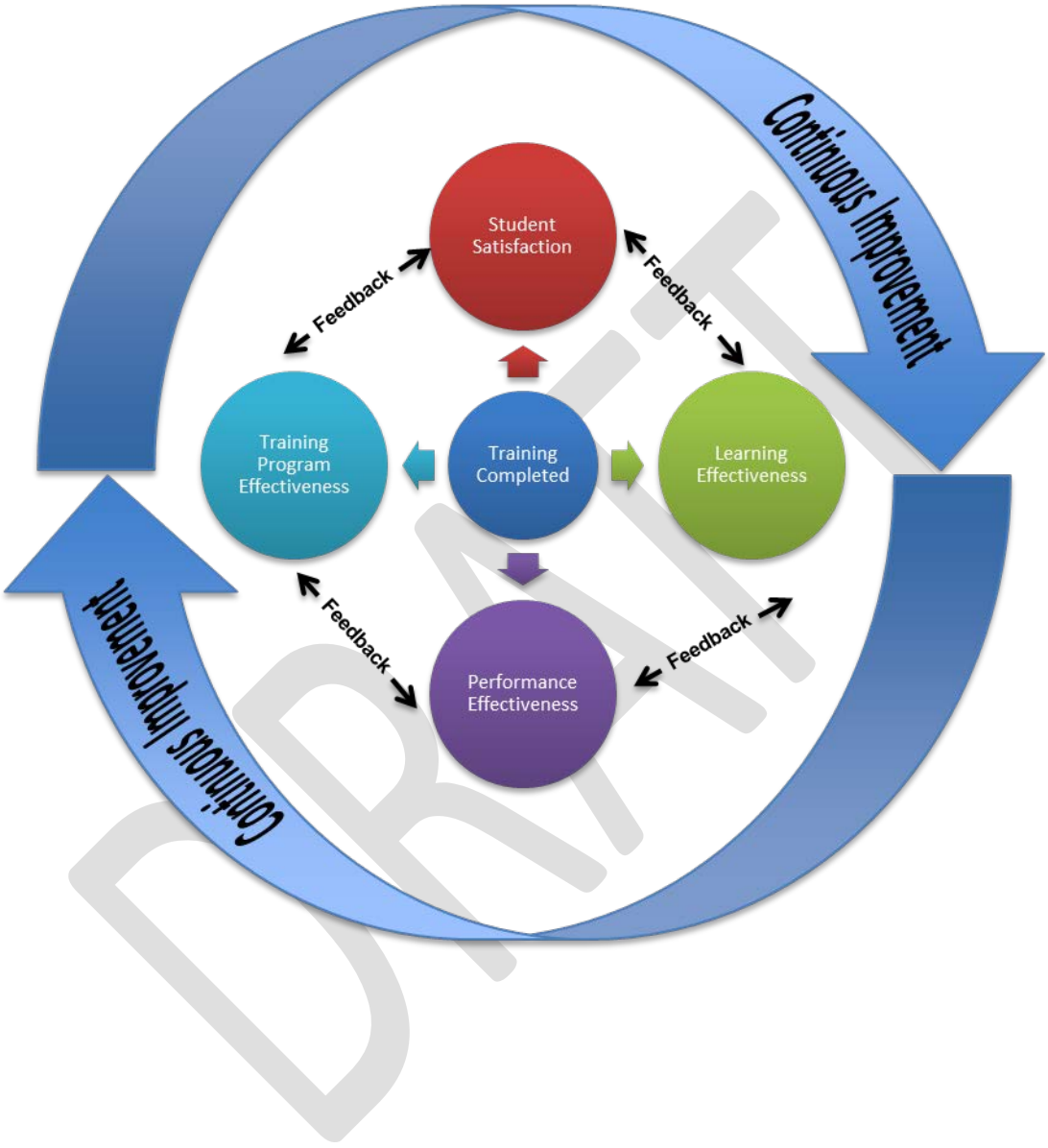
7.3.2.4 Assessing Training Program Effectiveness

This assessment is done by collecting data on whether the participants were satisfied with the deliverables of the training program, whether they learned something from the training and if they are able to apply those skills at their workplace

Evaluations can be difficult to undertake and hard to quantify. They can involve structured, follow-up interviews with students, their supervisors, and colleagues. They can involve comparison of outputs produced by a student both before and after training by a subject-matter expert. They can involve some form of benchmarking or evaluation of the particular training activity in relation to other options for a particular job performance measure. In all cases, they involve quantifying the value of resulting improvement in relation to the cost of training. Evaluations, properly designed, can help senior management officials to answer such hypothetical questions as: "Is it more cost-effective to devote limited training resources to the education of a single, newly-appointed information technology / cyber

DRAFT

security specialist in this organization, or to devote the same resources to Cybersecurity Essentials training of all employees in the organization?"; or "Is it a better return on investment to train 'front-end' systems designers and developers in building security rules commensurate with the sensitivity of the system, or to train 'back-end' users in compliance with currently existing system rules?"



DRAFT

7.4 Importance of Feedback

Critical to the evaluation process is that the feedback obtained be looped back into the training material. Thus, there is a continuous process of training, evaluation and then updating the training prior to the next presentation.

There are benefits that come with a good evaluation plan. First, evaluation ensures accountability which means that the evaluation ensures that training programs address the training gaps. Second, it assesses the cost and monies spent: evaluation ensures that the training programs are effective in improving the work quality, employee behavior, attitude and develop new skills and enhance old skills within a budget. Lastly, and, maybe most importantly, evaluations provide feedback to the trainer on the entire training process. Since evaluations access individuals at their work level, it is easier to understand and recognize the training loopholes and incorporate required changes in the training methodology.

DRAFT

Appendix A: Functions

This Appendix is designed to assist in determining which functions and roles should be identified as candidates for role-based training. Additionally, the outcomes for these functions are outlined.

Please note that the roles and Learning Objectives are guidelines, and can be tailored to meet the specific needs of an Agency or organization.

Functions associated with specific areas, such as "Collection and Targets", are not covered within this document. These exist but are considered highly specialized areas. For these functions, the identification of roles and outcomes can be selected by the Agency.

The format for this Appendix is as follows:

- **Function Area:** Identifies a security function area.
- **Roles Areas:** Identifies various roles that are covered by the function. These roles are guidelines and may exist under different names within a particular Agency.
- **Definition:** Provides a definition of the function.
- **Outcome(s):** Identifies the various outcomes that the training module should strive to meet for each of the functions and their associated roles.

DRAFT

INFORMATION TECHNOLOGY / CYBER
SECURITY TRAINING
Module for Functions

Function Area: **Oversight, Management and Support**

Role Areas:

- Legal Advice and Advocacy
- Strategic Planning and Policy Development
- Awareness, Education and Training
- Privacy
- Management
- Procurement
- Personnel Security
- Physical and Environmental Security
- Security Program Management

Definition — Provides oversight and support so that others may effectively conduct Cybersecurity work.

Learning Objectives —An individual should be able to successfully complete one or all of the following, depending on the role(s):

- Provide legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain.
- Advocate legal and policy changes and make a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.
- Apply knowledge of priorities to define an entity's direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest.
- Develop policy or advocate for changes in policy that will support new initiatives or required changes / enhancements.
- Conduct training of personnel within pertinent subject domains.
- Develop, plan, coordinate and evaluate training courses, methods, and techniques as appropriate.
- Oversees the Information Assurance (IA) program of an information system in or outside the network environment.
- Provides contractual, procurement and/or acquisition support for IA purchases.
- Manage information technology / cyber security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement emergency planning, security awareness, and other resources.
- Ensures that privacy impact assessments are conducted and appropriate controls are implemented.
- Ensures physical controls are correctly implemented.
- Provides personnel security policies, implements security controls and handles all personnel issues.

DRAFT

INFORMATION TECHNOLOGY / CYBER SECURITY TRAINING
Module for Functions

Function Area: **Securely Provision / Develop**

Role Areas:

- Information Assurance Compliance
- Software Assurance and Software Engineering
- Systems Security and Enterprise Architecture
- Technology Research and Development
- Systems Requirements Planning
- Test and Evaluation
- Systems Development

Definition — Addresses areas concerned with conceptualizing, designing, and building Information Technology systems, with the responsibility for some aspect of the systems' development.

Learning Objectives —An individual should be able to successfully complete one or all of the following, depending on the role(s):

- Oversee, evaluate and support the documentation, validation, and accreditation processes.
- Validate security compliance from internal and external perspectives.
- Develop, create, and write/code new (or modify existing) computer applications, software, or specialized utility programs.
- Develop system concepts and work on the capabilities phases of the systems development lifecycle.
- Translate technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.
- Conduct technology assessment and integration processes.
- Provide and support a prototype capability and evaluate its utility.
- Consult with customers to gather and evaluate functional requirements and translate these requirements into technical solutions.
- Provide guidance to customers about applicability of information systems to meet business needs.
- Develop and conduct tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics, including interoperability, of systems or elements of system incorporating information technology.
- Work on the development phases of the systems development lifecycle.

DRAFT

INFORMATION TECHNOLOGY / CYBER
SECURITY TRAINING
Curriculum Module for Functions

Function Area: **Operate and Maintain**

Role Areas:

- Data Administration
- Knowledge Management
- Information Systems Security Operations
- Customer Service and Technical Support
- Network Services
- System Administration
- System Security Analysis

Definition — Responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient information technology system performance and security.

Learning Objectives —An individual should be able to successfully complete one or all of the following, depending on the role(s):

- Develop and administer databases and/or data management systems that allow for the storage, query, and utilization of data.
- Oversee the information assurance program of an information system inside or outside the network environment.
- Manage and administer processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
- Addresses problems, installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries.
- Install, configure, test, operate, maintain, and manage the networks and their firewalls, including hardware and software, that permit the sharing and transmissions of information to support the security of the information and information systems.
- Install, configure, troubleshoot, and maintain server configurations to ensure their confidentiality, integrity, and availability.
- Manage accounts, firewalls, and patches.
- Create and administer access control, passwords and accounts.
- Conduct the integration / testing, operations and maintenance of system security.

DRAFT

INFORMATION TECHNOLOGY / CYBER
SECURITY TRAINING
Module for Functions

Function Area: **Protect**

Role Areas:

- Vulnerability Assessment and Management

Definition —Responsible for the identification and analysis of threats to internal information technology system or networks. Ensures that the security program is correctly implemented.

Learning Objectives —An individual should be able to successfully complete one of all of the following, depending on the role(s):

- Test, implement, deploy, maintain, and administer the infrastructure hardware and software that are required to effectively manage the computer network defense service to provider network and resources.
- Mange relevant security implications within the organization, specific program, or other area of responsibility. This includes strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.
- Conduct assessment of threats and vulnerabilities.
- Determine deviations from acceptable configurations, enterprise or local policy.
- Assess the level of risk.

DRAFT

INFORMATION TECHNOLOGY / CYBER
SECURITY TRAINING
Module for Functions

Function Area: **Defend**

Role Areas:

- Computer Network Defense Analysis
- Incident Response and Handling
- Computer Network Defense Infrastructure Support

Definition —Responsible for the identification, analysis and mitigation of threats to internal information technology system or networks.

Learning Objectives —An individual should be able to successfully complete one or all of the following, depending on the role(s):

- Ability to use defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems and networks from threats.
- Respond to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats.
- Develop and / or recommend appropriate mitigation countermeasures in operational and non-operational situations.

DRAFT

INFORMATION TECHNOLOGY / CYBER
SECURITY TRAINING
Module for Functions

Function Area: **Respond / Investigate**

Role Areas:

- Investigation
- Digital Forensics

Definition — Responsible for the investigation of cyber events and/or crimes of IT systems, networks, and safeguarding digital evidence.

Learning Objectives —An individual should be able to successfully complete one of all of the following, depending on the role(s):

- Apply tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection.
- Appropriately balance the benefits of prosecution versus intelligence gathering.
- Collect, process, preserve, analyze and present computer-related evidence in support of network vulnerability mitigation, and/or criminal fraud, counterintelligence or law enforcement investigations.
- Investigate and analyze all relevant response activities.

DRAFT

INFORMATION TECHNOLOGY / CYBER
SECURITY TRAINING
Module for Functions

Function Area: **Continuous Monitoring**

Role Areas:

- System Administration
- Vulnerability Assessment
- Trend Analysis
- Risk Management

Definition — Promotes near real-time risk management and ongoing system authorization.

Learning Objectives —An individual should be able to successfully complete one of all of the following, depending on the role(s):

- Monitor network to actively remediate unauthorized activities.
- Identify trends.
- Understand vulnerabilities and identify false negatives.

DRAFT

INFORMATION TECHNOLOGY / CYBER
SECURITY TRAINING
Module for Functions

Function Area: **Contingency Planning**

Role Areas:

- IT Disaster Recovery
- Enterprise Continuity
- Business Impact Analysis
- Training and Exercises
- First Response

Definition — Plan and prepare for response to an unplanned event, specific system failure, or disruption of operations.

Learning Objectives —An individual should be able to successfully complete one of all of the following, depending on the role(s):

- Use mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, and preservation of property.
- Use mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of information and maintain information technology / cyber security.
- Analyses business functions and IT requirements to determine impact to the organization and identify critical systems and applications.
- Conduct training and exercises of implemented plans and procedures to determine effectiveness.

DRAFT

Appendix B: Knowledge and Skills Catalog

K&S ID	Knowledge and Skills
	Overall
OV-1	Skill in communicating both orally and in writing
OV-2	Knowledge of fundamental Information Awareness concepts
OV-3	Knowledge of the Risk Management Framework and corresponding guidance
OV-4	Knowledge of the NIST SP 800-53 security controls and corresponding guidance
OV-5	Knowledge of technical documents and reports
OV-6	Skill in problem solving
OV-7	Knowledge of quality assurance
OV-8	Skill in reasoning techniques
OV-9	Knowledge of organizational awareness
OV-10	Knowledge of risks introduced by social media
OV-11	Knowledge of ethical standards
OV-12	Skill in ethical testing and implementation of security controls
OV-13	Knowledge of mathematical reasoning
	Advanced Network Technology and Protocols
ANTP-1	Knowledge of mobile technologies
ANTP-2	Skill in implementing and securing mobile technologies
ANTP-3	Skill in implementing advanced protocols
ANTP-4	Knowledge of security impacts of advanced network technology and protocols
ANTP-5	Knowledge of how advanced network services and protocols interact to provide network communications
	Architecture
ARCH-1	Knowledge of embedded systems
ARCH-2	Knowledge of digital rights management
ARCH-3	Knowledge of VPN security
ARCH-4	Skill in using VPN devices and encryption
ARCH-5	Knowledge of IT architecture concepts and frameworks
ARCH-6	Knowledge of parallel and distributed computing concepts
ARCH-7	Knowledge of remote access technology concepts
ARCH-8	Knowledge of the enterprise IT architecture
ARCH-9	Knowledge of communication methods, principles, and concepts that support the network infrastructure
ARCH-10	Knowledge of computer networking fundamentals
ARCH-11	Knowledge of the common networking protocols, services, and how they interact to provide network communications
ARCH-12	Knowledge of routing principles
ARCH-13	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not used standard IT) for safety, performance, and reliability
ARCH-14	Knowledge of enterprise messaging systems and associated software
ARCH-15	Knowledge of the organization's enterprise IT goals and objectives

DRAFT

ARCH-16	Skill in implementing the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise IT architecture
ARCH-17	Skill in analyzing and securing an enterprise architecture
ARCH-18	Knowledge of industry-standard and organizationally accepted security principles and methods
ARCH-19	Knowledge of engineering concepts
ARCH-20	Knowledge of structured analysis principles and methods
ARCH-21	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools
	COMPLIANCE
COMP-1	Skill in tracking and analyzing technical and legal trends that will impact cyber activities
COMP-2	Skill in determining impact of technology trend data on laws, regulations, and/or policies
COMP-3	Knowledge of International Traffic in Arms Regulations and relevance to cyber security
COMP-4	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, HIPAA, PCI-DSS, search and seizure laws, civil liberties and privacy laws, etc.), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Executive Orders, Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed
COMP-5	Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure
COMP-6	Skill in identifying the risks associated with social media
COMP-7	Knowledge of Personally Identifying Information (PII) and personal Payment Card Industry (PCI) data security standards
COMP-8	Skill in developing and executing test methodologies to ensure compliance to directives (Policy and/or technical)
COMP-9	Knowledge of rationale for organizationally defined auditable events
COMP-10	Knowledge of technical and legal trends that impact cyber activities
	COMPUTER NETWORK DEFENSE
CND – 1	Knowledge of Computer Network Defense and vulnerability assessment tools, including open source tools, and their capabilities
CND – 2	Knowledge of intrusion detection and prevention system tools and applications
CND – 3	Knowledge of Contenet dev
CND – 4	Knowledge of the types of intrusion detection and prevention system hardware and software
CND – 5	Skill in handling malware
CND-6	Skill in detecting host and network-based intrusions via intrusion detection and prevention, and other network monitoring tools
CND – 7	Skill in mimicking threat behaviors
CND – 8	Skill in tuning security monitoring sensors
CND – 9	Knowledge of Insider Threat investigations, reporting, investigative tools, and laws/regulations
CND – 10	Knowledge of computer network operations methodologies, including analysis and exploitation
CND – 11	Knowledge of common adversary capabilities, tactics, techniques, and procedures in assigned area of responsibility
CND – 12	Knowledge of Defense-In-Depth principles and network security architecture
CND – 13	Skill in collecting data from a variety of Computer Network Defense resources
CND-14	Skill in protecting a network against malware
CND – 15	Knowledge of Computer Network Defense policies, procedures, and regulations

DRAFT

CND – 16	Knowledge of the common attack vectors on the network layer
CND – 17	Knowledge of different classes of attacks
CND – 18	Knowledge of operational threat environments
CND – 19	Knowledge of malware analysis concepts and methodology
CND – 20	Knowledge of general attack stages
CND – 21	Skill in deep analysis of captured malicious code
CND – 22	Knowledge of malware analysis and tools
CND – 23	Knowledge of virtual machine aware malware, debugger aware malware, and packing
CND -24	Skill in analyzing anomalous code as malicious or benign
CND – 25	Skill in identifying obfuscation techniques and removing the malware
CND-26	Skill in conducting investigations and developing comprehensive reports
CND – 27	Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures
CND-28	Skill in malware analysis
CND-29	Knowledge of the CND Service Provider reporting structure and processes within one's own organization
CND-30	Skill in de-conflicting cyber operations and activities from operational activities
	CONFIGURATION MANAGEMENT
CM – 1	Knowledge of secure configuration management techniques
CM-2	Skill in developing configuration baselines per appropriate hardening guides
CM-3	Skill in documenting configuration settings
CM-4	Skill in security impact analysis of changes to the configuration
CM-5	Knowledge of configuration change control
CM-6	Knowledge of access restrictions for change
CM-7	Skill in developing configuration management policy and procedures
CM-8	Skill in maintaining configuration baseline of the information system
CM-9	Knowledge of information system component inventory
CM-10	Skill in developing information system component inventory
CM-11	Knowledge of configuration management plan and how it is used
CM-12	Skill in developing configuration management plan
CM-13	Knowledge of configuration management requirements for developers
CM-14	Skill in implementing configuration change controls
CM-15	Skill in implementing configuration management plan
	CRYPTOGRAPHY AND ENCRYTION
CR -1	Knowledge of encryption methodologies
CR – 2	Knowledge of encryption algorithms
CR -3	Knowledge of cryptography
CR-4	Knowledge of cryptographic implementation
CR-5	Knowledge of certificate management infrastructures
CR-6	Skill in encryption methodologies
CR-7	Skill in cryptography implementation
CR-8	Skill in decryption if digital data
CR-9	Skill in one way hash functions

CR-10	Knowledge of computer algorithms
CR-11	Skills in implementing the FIPS validated cryptography
CR-12	Skill in implementing and maintaining transmission confidentiality and integrity
CR-13	Skill in implementing NSA approved cryptography
CR-14	Knowledge of FIPS validated cryptography
CR-15	Knowledge of NSA approved cryptography
	DATA SECURITY
DS-1	Skill in analyzing network traffic capacity and performance characteristics
DS-2	Knowledge of data administration and data standardization policies and standards
DS-3	Knowledge of data mining and data warehousing principles
DS-4	Knowledge of sources, characteristics, and uses of the organization's data assets
DS-5	Knowledge of the capabilities and functionality associated with various technologies for organizing and managing information
DS-6	Knowledge of the characteristics of physical and virtual data storage media
DS-7	Skill in developing data dictionaries
DS-8	Skill in developing data repositories
DS-9	Skill in data mining techniques
DS-10	Knowledge of database theory
DS-11	Skill in data reduction
DS-12	Skill in the interpretation and incorporation of data from multiple tool sources
DS-13	Knowledge of complex data structures
DS-14	Knowledge of computer programming principles such as object-oriented design
DS-15	Skill in Data Loss Prevention technologies (DLP)
DS-16	Knowledge of logical access to system functions
DS-17	Skill in enforcing logical access controls
DS-18	Skill in enforcement of information flow policies
	DATABASE
DB-1	Skill in allocating storage capacity in the design of database management systems
DB-2	Skill in designing databases
DB-3	Skill in optimizing database performance
DB-4	Knowledge of database management systems, query languages, table relationships, and views
DB-5	Knowledge of database systems
DB-6	Knowledge of query languages
DB-7	Skill in conducting queries and developing algorithms to analyze data structures
DB-8	Skill in generating queries and reports
DB-9	Skill in maintaining databases
DB-10	Skill in implementing backup plans
DB-11	Skill in implementing maintenance plans
	DIGITAL FORENSICS
DF-1	Knowledge of seizing and preserving digital evidence
DF-2	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data

DRAFT

DF-3	Skill in setting up a forensic workstation
DF-4	Knowledge of basic concepts and practices of processing digital forensic data
DF-5	Skill in analyzing memory dumps to extract information
DF-6	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools
DF-7	Knowledge of server diagnostic tools and fault identification techniques
DF-8	Skill in preserving evidence integrity according to standard operating procedures or national standards
DF-9	Knowledge of investigative implications of hardware, Operating Systems, and network technologies
DF-10	Knowledge of types and collection of persistent data
DF-11	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files
DF-12	Skill in identifying and extracting data of forensic interest in diverse media
DF-13	Skill in using forensic tool suites
DF-14	Knowledge of types of digital forensics data and how to recognize them
DF-15	Knowledge of deployable forensic software to perform forensic imaging remotely
DF-16	Skill in conducting forensic analyses in multiple operating system environments
DF-17	Skill in decrypting digital data collections
DF-18	Skill in identifying forensic footprints
DF-19	Knowledge of data carving tools and techniques
DF-20	Knowledge of anti-forensics tactics, techniques, and procedures
DF-21	Knowledge of common forensics tool configuration and support applications
DF-22	Skill in analyzing volatile data
DF-23	Knowledge of legal governance related to admissibility, such as Federal Rules of Evidence
DF-24	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data
DF-25	Knowledge of electronic evidence law
DF-26	Knowledge of legal rules of evidence and court procedure
DF-27	Knowledge of file system geometry in multiple operating systems
DF-28	Knowledge of mobile device forensics
DF-29	Knowledge of image acquisition and validation
DF-30	Skill in retrieving forensic information from information system backups
DF-31	Skill in recognizing security incident trends in forensic data
	EMERGING TECHNOLOGIES
ET-1	Knowledge of new and emerging IT and information technology / cyber security technologies
ET-2	Knowledge of new technological developments in server administration
ET-3	Knowledge of the capabilities and functionality associated with various content creation technologies
ET-4	Knowledge of the capabilities and functionality of various collaborative technologies
ET-5	Skill in applying and incorporating IT technologies into proposed solutions
ET-6	Skill in the determination of the validity of technology trend data
ET-7	Knowledge of emerging computer-based technology that have potential for exploitation by adversaries
ET-8	Knowledge of industry indicators useful for identifying technology trends
ET-9	Knowledge of products and nomenclature of major vendors and how differences affect exploitation/vulnerabilities

DRAFT

ET-10	Knowledge of emerging security issues, risks, and vulnerabilities
ET-11	Knowledge of cloud computing environments and the risks
	ENTERPRISE CONTINUITY
ECP-1	Knowledge of disaster recovery and continuity of operations plans
ECP-2	Knowledge of enterprise continuity response program, roles, and responsibilities
ECP-3	Skill in developing disaster recovery and continuity of operations plans
ECP-4	Skill in executing disaster recovery and continuity of operations plans
ECP-5	Knowledge of enterprise continuity planning
ECP-6	Skill in conducting Business Impact Assessments
ECP-7	Skill in developing disaster recovery and continuity of operations strategies
ECP-8	Skill in developing enterprise business continuity plans
ECP-9	Skill in exercising and maintaining enterprise business continuity plans
ECP-10	Skill in developing, testing, and implementing network infrastructure contingency and recovery plans
ECP-11	Skill in performing damage assessments
ECP-12	Skill in testing use of alternate storage site
ECP-13	Skill in testing use of alternate processing site
ECP-14	Knowledge of alternate telecommunication services for primary and alternate processing or storage sites
ECP-15	Knowledge of location of information system backups and their recovery procedures
ECP-16	Knowledge of activities involved in information system recovery and reconstitution
ECP-17	Skill in performing activities involved in information system recovery and reconstitution
ECP-18	Skill in assessing and employing organization defined security controls at alternate work sites
	IDENTITY MANAGEMENT / PRIVACY
IM-1	Knowledge of access authentication methods
IM-2	Knowledge of network access, identity and access management
IM-3	Knowledge of policy-based and risk adaptive access controls
IM-4	Skill in applying host/network access controls
IM-5	Skill in developing and applying security system access controls
IM-6	Skill in maintaining directory services
IM-7	Knowledge of organizational IT user security policies
IM-8	Skill in identifying privacy issues and associated mitigation
IM-9	Knowledge of collection, use, maintenance and sharing of PII
IM-10	Skill in conducting Privacy Impact Assessment
IM-11	Skill in monitoring and auditing privacy controls and internal privacy policies
	INCIDENT MANAGEMENT
IR-1	Knowledge of procedures used for documenting and querying reported incidents
IR-2	Knowledge of incident categories, incident responses, and timelines for responses
IR-3	Knowledge of incident response and handling methodologies
IR-4	Skill in recovering failed servers
IR-5	Skill in using incident handling methodologies
IR-6	Knowledge of enterprise incident response program, roles, and responsibilities
IR-7	Knowledge of root cause analysis for incidents

IR-8	Skill in performing root cause analysis for incidents
IR-9	Skill in isolating compromised systems
IR-10	Knowledge in performing traffic analysis
IR-11	Knowledge of secure transfer of evidence to forensics
IR-12	Skill in security monitoring to determine possible incidents
IR-13	Skill to correlate and combine data to develop information about the capabilities, intent, and operations of criminal and/or adversary organizations
IR-14	Skill in recognizing and categorizing types of vulnerabilities and associated attacks
IR-15	Skill in performing damage assessments from incidents
IR-16	Knowledge of processes for reporting security related incidents
IR-17	Skill in monitoring and evaluating security incident trends
IR-18	Knowledge that security incident trends exist
IR-19	Skill in providing incident response support
IR-20	Knowledge of security alerts, advisories, and directives
	INDUSTRIAL CONTROL SYSTEMS
ICS-1	Knowledge of risk(s) specific to Industrial Control Systems (ICS)
ICS-2	Knowledge of ICS unique performance and reliability requirements
ICS-3	Skill in restricting logical access to the ICS network and network activity
ICS-4	Skill in restricting physical access to the ICS network and devices
ICS-5	Skill in protecting individual ICS components from exploitation
ICS-6	Skill in maintaining functionality during adverse conditions
ICS-7	Skill in restoring ICS after incident quickly
	INFORMATION ASSURANCE
IA-1	Knowledge of Security Assessment and Authorization process
IA-2	Knowledge of IA principles used to manage risks related to the use, processing, storage, and transmission of information or data
IA-3	Knowledge of IA principles and methods that apply to software development
IA-4	Knowledge of IA principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation)
IA-5	Knowledge of security management
IA-6	Skill in designing security controls based on IA principles and tenets
IA-7	Skill in determining how an information system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes
IA-8	Skill in securing network communications
IA-9	Knowledge of various means to validate information system input
	WEB SECURITY
WT-1	Knowledge of web services
WT-2	Knowledge of web collection, session management, searching/analyzing techniques, tools, and cookies
WT-3	Knowledge of web filtering technologies
WT-4	Knowledge of OWASP, ISO, and other standards relating to web based applications
WT-5	Skill in building, designing and testing the security of web applications and web services
WT-6	Knowledge of common web application attack vectors

DRAFT

WT-7	Knowledge of user input validation techniques for web applications
WT-8	Skill in performing web applications testing
WT-9	Knowledge of web applications firewalls
WT-10	Skill in training authorized individuals to ensure that publicly accessible information does not contain nonpublic information
	INFORMATION SYSTEMS
SI-1	Knowledge of how system components are installed, integrated, and optimized
SI-2	Knowledge of principles and methods for integrating server components
SI-3	Knowledge of technology integration processes
SI-4	Skill in designing the integration of hardware and software solutions
SI-5	Knowledge of operating systems
SI-6	Knowledge of server and client operating systems
SI-7	Knowledge of systems administration concepts
SI-8	Skill in system administration for operating systems
SI-9	Knowledge of file system implementations
SI-10	Knowledge of virtualization technologies and virtual machine development and maintenance
SI-11	Knowledge of command lines
SI-12	Skill in identifying, modifying, and manipulating applicable system components
SI-13	Skill in reading, interpreting, writing, modifying, and executing simple scripts on systems that perform tasks like parsing large data files, automating manual tasks, and fetching/processing remote data
SI-14	Skill in operating virtual machines
SI-15	Knowledge of troubleshooting basic systems and operating system related issues
SI-16	Knowledge of operating system structure and internals
SI-17	Skill in utilizing virtual networks for testing
SI-18	Knowledge of operating system's ports and services
SI-19	Skill in installing and configuring virtual machines
SI-20	Skill in matching the appropriate knowledge repository technology for a given application or environment
SI-21	Knowledge of “knowledge base” capabilities in identifying the solutions to less common and more complex system problems
SI-22	Skill in conducting knowledge mapping
SI-23	Skill in conducting open source research for troubleshooting client-level problems
SI-24	Skill in using knowledge management technologies
SI-25	Knowledge of Storage Area Networks
SI-26	Knowledge of external information system impact to the security baseline
SI-27	Knowledge of information backed up and schedule of information system backup
SI-28	Knowledge of identification and authentication techniques
SI-29	Skills in implementing identification and authentication through various means
SI-30	Knowledge of various types of Spam and other attack methodologies
SI-31	Skill in implementing protective measures for various types of Spam and other attacks
	IT SYSTEMS AND OPERATIONS
ITOS-1	Knowledge of circuit analysis
ITOS-2	Knowledge of microprocessors

DRAFT

ITOS-3	Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system
ITOS-4	Knowledge of basic physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage)
ITOS-5	Skill in physically assembling and disassembling PCs
ITOS-6	Skill in conducting information searches
ITOS-7	Skill in the basic operation of computers
ITOS-8	Skill in processing collected data for follow-on analysis
ITOS-9	Knowledge of storage capacity
ITOS-10	Knowledge of capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware
ITOS-11	Knowledge of network hardware devices and functions
ITOS-12	Skill in implementation of auditable events
ITOS-13	Skill in configuring and utilizing hardware-based computer protection components
ITOS-14	Knowledge of electrical engineering as applied to computer architecture, including circuit boards, processors, chips, and associated computer hardware
ITOS-15	Skill in managing information system accounts and their access to information systems
ITOS-16	Skill in determining organizationally defined auditable events
ITOS-17	Skill in handling audit processing failures
ITOS-18	Knowledge of audit records and the protection thereof
ITOS-19	Skill in implementing the protection of audit records
ITOS-20	Skill in tracking use of software and documentation protected by licenses
ITOS-21	Skill in monitoring policy compliance for user-installed software
ITOS-22	Skill in protecting the confidentiality of transmitted information
ITOS-23	Knowledge that information must be protected at rest and during transmission
ITOS-24	Skill in performing information system backups
ITOS-25	Knowledge of processes to maintain the system and user documentation
ITOS-26	Skill in employing audit reduction and report generation capabilities
ITOS-27	Knowledge of audit reduction and report generation
	IT SECURITY AWARENESS AND TRAINING
SAT-1	Knowledge of multiple cognitive domains and appropriate tools and methods for learning in each domain
SAT-2	Skill in developing curriculum that speaks to the topic at the appropriate level for the target audience
SAT-3	Skill in identifying upcoming IA topics to ensure awareness
SAT-4	Skill in preparing and delivering education and awareness briefings to ensure that systems, network, and data users are aware of and adhere to systems security policies and procedures
SAT-5	Skill in identifying gaps in technical capabilities
SAT-6	Knowledge of academic institutions dealing with cyber security issues
SAT-7	Skill in developing and executing technical training programs and curricula
SAT-8	Skill in maintaining and retaining security training records
SAT-9	Skill in developing and executing tests of the contingency plans
SAT-10	Knowledge of requirements for developer provided information technology / cyber security training
SAT-11	Skill in training individuals in contingency planning
SAT-12	Skill in training individuals in incident response procedures
	MANAGEMENT

DRAFT

PM-1	Knowledge of resource management principles and techniques
PM-2	Knowledge of information technology / cyber security program management and project management principles and techniques
PM-3	Knowledge of risk management principles
PM-4	Knowledge of budgeting process to ensure security is addressed
PM-5	Skill in the development, implementation and maintenance of systems security plan
PM-6	Skill in the development of security policies and procedures
PM-7	Skill in the implementation of security policies
PM-8	Knowledge of the various security policies and plans
PM-9	Knowledge of external organizations dealing with cyber security issues
PM-10	Knowledge of how information needs are translated, tracked, and prioritized across the extended enterprise
PM-11	Knowledge of Privacy Issues and Mitigation
PM-12	Knowledge of federal reporting principles, policies, procedures, and vehicles, including report formats, reportability criteria (requirements and priorities), dissemination practices, and legal authorities and restrictions
PM-13	Knowledge of the structure and intent of concept operation and rules of engagement
PM-14	Knowledge of the organization's core business/mission processes
PM-15	Knowledge of the risks associated with social media
PM-16	Skill in the measuring and reporting of intellectual capital
PM-17	Knowledge of organization's evaluation and validation requirements
PM-18	Knowledge of established trust relationships with other organizations owning, operating, and/or maintaining external information systems
PM-19	Knowledge that security training records must be retained as well as the retention period
PM-20	Knowledge of organizationally defined auditable events
PM-21	Knowledge of contract agreements and copyright laws for software and associated documentation
PM-22	Knowledge of policies related to user-installed software
PM-23	Skill in understanding the IT Contingency Plan and its associated activities
PM-24	Skill ensuring the information system backup policy is enforced
PM-25	Knowledge of incident response support resources roles
PM-26	Knowledge of incident response plan
PM-27	Knowledge of applicable processes for downgrading media
PM-28	Knowledge of information system security architecture
PM-29	Skill in integrating and supporting information system security architecture
PM-30	Knowledge and understanding of security categorization for information systems
PM-31	Knowledge and understanding information handling and retention policy
PM-32	Knowledge of capital investment with regards to information assurance
PM-33	Skill in developing and implementing appropriate security agreements, such as Memorandum of Agreements, SLAs, etc.
PM-34	Knowledge of Access Control policies, procedures and security controls
PM-35	Knowledge of Contingency Plans and associated guidance
PM-36	Knowledge of Identification and Authentication policies, procedures and security controls
PM-37	Knowledge of Systems Acquisition policies, procedures and associated guidance
PM-38	Knowledge of System and Communications Protection policies, procedures and security controls

DRAFT

PM-39	Knowledge of System Integrity policies, procedures and security controls
PM-40	Knowledge of Audit and Accountability policies, procedures and security controls
PM-41	Knowledge of Incident Response policies, procedures and security controls
PM-42	Knowledge of Maintenance policies, procedures and security controls
PM-43	Knowledge of Maintenance associated guidelines and log implementation
PM-44	Knowledge of Media Protection policies, procedures, associated guidelines and security controls
PM-45	Knowledge of Physical and Environmental policies, procedures and security controls
PM-46	Knowledge of Personnel Security policies, procedures and security controls
PM-47	Knowledge of Security Assessment and Authorization policies, procedures and security controls
PM-48	Knowledge Configuration Management policies, procedures and security controls
PM-49	Knowledge of Risk Management policies, procedures and security controls
PM-50	Knowledge of Security Planning policies, procedures and associated guidelines
PM-51	Knowledge of Security Awareness and Training policies, procedures and associated guidance
PM-52	Knowledge of Return on Investment (ROI) analysis
PM-53	Skill in analyzing return on investment (ROI)
	MODELING AND SIMULATION
MS-1	Skill in creating and utilizing mathematical or statistical models
MS-2	Skill in developing data models
MS-3	Skill in the use of design modeling
	NETWORK AND TELECOMMUNICATIONS SECURITY
NTS-1	Skill in conducting server planning, management, and maintenance
NTS-2	Skill in correcting physical and technical problems which impact server performance
NTS-3	Skill in diagnosing connectivity problems
NTS-4	Skill in diagnosing failed servers
NTS-5	Skill in testing and configuring network hardware and peripherals
NTS-6	Skill in using network management tools to analyze network traffic patterns
NTS-7	Knowledge of the capabilities of different electronic communication systems and methods
NTS-8	Knowledge of the range of existing networks
NTS-9	Knowledge of network systems management principles, models, methods and tools
NTS-10	Skill in configuring and utilizing network protection components
NTS-11	Knowledge of organization's LAN/WAN pathways and other telecommunication pathways
NTS-12	Knowledge of how network services and protocols interact to provide network communications
NTS-13	Knowledge of local area and wide area networking principles and concepts including bandwidth management
NTS-14	Knowledge of network protocols
NTS-15	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs
NTS-16	Knowledge of how traffic flows across the network
NTS-17	Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, hubs, and switches
NTS-18	Skill in network mapping and recreating network topologies
NTS-19	Skill in using sub-netting tools

DRAFT

NTS-20	Knowledge of common network tools
NTS-21	Knowledge of host/network access controls
NTS-22	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins
NTS-23	Knowledge of IT security principles and methods
NTS-24	Knowledge of current industry methods for evaluating, implementing, and disseminating network security assessment, monitoring, detection and remediation tools and procedures utilizing standards-based concepts and capabilities
NTS-25	Knowledge of network traffic analysis methods
NTS-26	Knowledge of network security design tools, methods, and techniques
NTS-27	Knowledge of the CND Service Provider reporting structure and processes within one's own organization for network incidents
NTS-28	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities
NTS-29	Skill in developing and deploying intrusion detection / protection signatures
NTS-30	Skill in discerning the protection needs (i.e., security controls) of networks
NTS-31	Skill in implementing, maintaining, and improving established network security practices
NTS-32	Knowledge of front-end collection systems, including network traffic collection, filtering, and selection
NTS-33	Knowledge of security event correlation tools
NTS-34	Knowledge of current and emerging threats/threat vectors
NTS-35	Knowledge of basic network administration, and network hardening techniques
NTS-36	Knowledge of network security architecture concepts including topology, protocols, components, and principles
NTS-37	Skill in reading and interpreting intrusion detection / protection signatures
NTS-38	Knowledge of intrusion detection / protection signature implementation impact
NTS-39	Skill in enforcement of policies
NTS-40	Knowledge of packet-level analysis
NTS-41	Knowledge of telecommunications concepts
NTS-42	Knowledge of basic concepts, terminology, and operations of a wide range of communications media
NTS-43	Knowledge of different types of network communication
NTS-44	Knowledge of the nature and function of the relevant information structure
NTS-45	Knowledge of Voice over IP (VoIP)
NTS-46	Knowledge of mobile communications architecture
NTS-47	Knowledge of transmission methods
NTS-48	Skill in establishing a routing schema
NTS-49	Skill in applying network programming towards client/server model
NTS-50	Knowledge of organization's LAN/WAN pathways
NTS-51	Skill in testing alternate telecommunication services
NTS-52	Knowledge of collaborative computing devices and their risk to the information system security baseline
	PERSONNEL SECURITY
PS-1	Knowledge of human-computer interaction principles
PS-2	Knowledge of and promotion of general awareness regarding the use of social engineering techniques
PS-3	Knowledge of Privacy Impact Assessments
PS-4	Knowledge of operations security

DRAFT

PS-5	Skill in assigning position descriptions
PS-6	Knowledge of hiring, termination, and transfer actions impacting information systems access
PS-7	Knowledge of third party access requirements
PS-8	Knowledge of ethical testing
PS-9	Knowledge of social dynamics of computer attackers in a global context
PS-10	Knowledge of threat list countries' cyber capabilities, intent, opportunities, and presence
PS-11	Knowledge of correct behavior for information system use
PS-12	Skill in writing the rules that govern correct behavior for information system use
	PHYSICAL AND ENVIRONMENTAL SECURITY
PES-1	Knowledge of physical access controls
PES-2	Skill in implementing various physical access controls
PES-3	Skill in monitoring physical access
PES-4	Knowledge of emergency power
PES-5	Knowledge of fire protection systems
PES-6	Knowledge of environmental controls and hazards
PES-7	Skill in configuring ports and input/output devices
PES-8	Knowledge of physical controls for datacenter(s)
PES-9	Skill in implementing physical controls for areas housing computer systems and networks
	PROCUREMENT
PROC-1	Knowledge of applicable business processes and operations of customer organizations
PROC-2	Knowledge of capabilities and requirements analysis
PROC-3	Knowledge of system software and organizational design standards, policies, and authorized approaches relating to system design
PROC-4	Skill in conducting capabilities and requirements analysis
PROC-5	Skill in interpreting and translating customer requirements into operational cyber actions
PROC-6	Knowledge of secure acquisitions
PROC-7	Knowledge of Export Control regulations and responsible Federal Organizations for the purposes of reducing supply chain risk
PROC-8	Knowledge of critical IT procurement requirements
PROC-9	Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes)
PROC-10	Skill in evaluating the trustworthiness of the supplier and/or product
PROC-11	Knowledge of processes to allocate resources in business process planning
PROC-12	Skill in ensuring the proper allocations of resources in business process planning
	SECURITY RISK MANAGEMENT
RM-1	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems
RM-2	Skill to identify systemic security issues based on the analysis of vulnerability and configuration data
RM-3	Knowledge of application vulnerabilities
RM-4	Knowledge of penetration testing principles, tools, and techniques
RM-5	Knowledge of system and application security threats and vulnerabilities
RM-6	Knowledge of network security threats and vulnerabilities
RM-7	Skill in assessing the robustness of security systems and designs

RM-8	Skill in designing countermeasures to identified security risks
RM-9	Skill in evaluating the adequacy of security designs
RM-10	Skill in performing packet-level analysis
RM-11	Skill in the use of penetration testing tools and techniques
RM-12	Skill in using protocol analyzers
RM-13	Skill in applying white hat hacking/security auditing techniques, procedures, and tools
RM-14	Skill in using network analysis tools to identify vulnerabilities
RM-15	Skill in utilizing exploitation tools to identify system/software vulnerabilities
RM-16	Skill in utilizing network analysis tools to identify software communications vulnerabilities
RM-17	Knowledge of reverse engineering concepts and techniques
RM-18	Knowledge of how different file types can be used for anomalous behavior
RM-19	Knowledge of measures or indicators of system performance and availability
RM-20	Knowledge of performance tuning tools and techniques
RM-21	Skill in identifying and anticipating server performance, availability, capacity, or configuration problems
RM-22	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance relative to the goals of the system
RM-23	Skill in monitoring and optimizing server performance
RM-24	Skill in conducting audits or reviews of technical systems
RM-25	Skill in risk management processes, including steps and methods for assessing risk
RM-26	Knowledge of organization's risk tolerance and/or risk management approach
RM-27	Knowledge of supply chain risk management processes and practices
RM-28	Knowledge of risk threat assessment
RM-29	Skill in implementing IT supply chain security/risk management policies, requirements, and procedures
RM-30	Knowledge of Risk Management Framework
RM-31	Skill in creating policies that reflect system security goals
RM-32	Skill in correlation of data to develop information about the capabilities, intent, and operations of criminal and/or adversary organizations
RM-33	Knowledge of hacking methodologies
RM-34	Skill in analyzing audit records
	SOFTWARE
SW-1	Knowledge of software debugging principles
SW-2	Knowledge of software design tools, methods, and techniques
SW-3	Skill in conducting software debugging
SW-4	Skill in developing applications that can log errors, exceptions, and application faults and logging
SW-5	Skill in using code analysis tools to eradicate bugs
SW-6	Skill in writing kernel level applications
SW-7	Knowledge of Middleware
SW-8	Knowledge of debugging procedures and tools
SW-9	Skill in developing technical design documentation
SW-10	Skill in developing software design documentation
SW-11	Knowledge of software development models
SW-12	Knowledge of software engineering

DRAFT

SW-13	Skill in configuring and optimizing software
SW-14	Knowledge of software quality assurance process
SW-15	Knowledge of secure software deployment methodologies, tools and practices
SW-16	Skill in configuring and utilizing software-based computer protection tools
SW-17	Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams
SW-18	Skill in tailoring code analysis for application-specific concerns
SW-19	Knowledge of low-level computer languages
SW-20	Knowledge of programming language structures and logic
SW-21	Skill in writing code in a modern programming language
SW-22	Knowledge of language command line(s)
SW-23	Knowledge of interpreted and compiled computer language
SW-24	Knowledge of secure coding techniques
SW-25	Skill in using binary analysis tools
SW-26	Skill in reading Hexadecimal data
SW-27	Skill in identifying common encoding techniques
SW-28	Knowledge of system security plans
SW-29	Skill in the implementation of security plans
SW-30	Knowledge of software, firmware, and information integrity verification tools
SW-31	Skill in employing software, firmware, and information integrity verification tools
SW-32	Knowledge of software assurance
	SYSTEMS AND APPLICATION SECURITY
SAS-1	Knowledge of server administration and systems engineering theories, concepts, and methods
SAS-2	Knowledge of systems lifecycle management principles, including software security and usability
SAS-3	Knowledge of the operations and processes for diagnosing common or recurring system problems
SAS-4	Knowledge of the systems engineering process
SAS-5	Knowledge of the type and frequency of routine maintenance needed to keep equipment functioning properly
SAS-6	Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation
SAS-7	Skill in installing computer and server upgrades
SAS-8	Knowledge of the life cycle process
SAS-9	Knowledge of systems diagnostic tools and fault identification techniques
SAS-10	Knowledge of systems testing and evaluation methods
SAS-11	Skill in applying organization-specific systems analysis principles and techniques
SAS-12	Skill in conducting test events
SAS-13	Skill in designing a data analysis structure
SAS-14	Skill in determining an appropriate level of test rigor for a given system
SAS-15	Skill in developing operations-based testing scenarios
SAS-16	Skill in systems integration testing
SAS-17	Skill in writing test plans
SAS-18	Skill in evaluating test plans for applicability and completeness

DRAFT

SAS-19	Skill in secure test plan design
SAS-20	Knowledge of known system and application vulnerabilities from alerts, advisories, errata, and bulletins
SAS-21	Knowledge of information technology / cyber security systems engineering principles
SAS-22	Knowledge of system and application security principles and methods
SAS-23	Knowledge of current industry methods for evaluating, implementing, and disseminating IT security assessment, monitoring, detection and remediation tools and procedures utilizing standards-based concepts and capabilities
SAS-24	Knowledge of security system design tools, methods, and techniques
SAS-25	Knowledge of the Service Provider reporting structure and processes within one's own organization
SAS-26	Skill in discerning the protection needs (i.e., security controls) of information systems
SAS-27	Knowledge of system and application security event correlation tools
SAS-28	Knowledge of software related IT security principles and methods
SAS-29	Knowledge of basic system administration, and operating system hardening techniques
SAS -30	Skill in basic system administration, and operating system hardening techniques
SAS-31	Knowledge of signature implementation impact
SAS-32	Knowledge of malicious code protection mechanisms
SAS-33	Skill in implementing malicious code protection
SAS-34	Knowledge of current and emerging threats/threat vectors against information systems and applications

DRAFT

Appendix C: Roles

This Appendix is designed to assist in determining which competency and associated Knowledge and Skills are required by a particular role. Knowledge is the theoretical or practical understanding of the competency.

Please note that there is no hierarchy within the Knowledge and Skills. No Knowledge or Skill is of greater value than another. The first Knowledge and Skill listed within the knowledge unit has no order preference on those Knowledge and Skills listed elsewhere in list.

Additionally, the generic roles and job titles used within this Appendix may or may not be the same as the roles or job titles used by and individual Agency or organization. The ones used within this Appendix are a sample of current jobs / roles within various Federal Organizations and organizations at the time of publication. Using the competencies and functions, each of these samples can be tailored to meet the roles within a specific Agency.

Roles for highly specialized areas are not covered. The roles, and associated knowledge and skills should be tailored by the Agency.

All roles should have training on the Overall Knowledge and Skills as described within Appendix C, Competencies, Knowledge and Skills Catalog. These are the fundamental basis of knowledge/skills required for all jobs and roles.

Abilities are not covered in this document. Abilities are the specific skills that are obtained while on the job using the knowledge and skills that were obtained during the role-based security training. Therefore, it is assumed that abilities cannot be taught, but rather acquired throughout the employee's career.

The format is as follows:

- **Function Area**: This area corresponds with *Appendix A: Function Areas*. Appendix A provides a general description of the area and the Learning Objectives for those functions. The roles described within this appendix are within a function.
- **Role Area**: This describes the overall role.
- **Roles**: A list of various job titles / roles is provided to assist in determining who should receive this role based training
- **Responsibility**: Defines the activities and or responsibilities of that particular role
- **Knowledge Unit**: Identifies the competencies associated with the role. The entire listing of the knowledge units and their associated knowledge and skills are located in *Appendix C: Knowledge and Skills Catalog*.
- **Corresponding Knowledge and Skills Table**: This table provides a breakdown of the specific knowledge unit, the corresponding knowledge and skills to each competency. Each role has various knowledge units associated with it. There are 4 differing areas that correspond with the job title to allow for further tailoring of role-based security training to better match with the job function. These areas are defined as follows:

DRAFT

- **Manage** – those knowledge and skills particular to those employees who are responsible for management (e.g., managers, team leads, project managers)
- **Design** – those knowledge and skills particular to those employees who are responsible for design activities (e.g., system developers, engineers)
- **Implement** – those knowledge and skills particular to those employees who execute implementation (e.g., system administrators, network administrators)
- **Evaluate** – those knowledge and skills particular to evaluation activities (e.g., testers, security analysts)

To assist with the tailoring of the training or to identify courses / modules that may have already been developed, there is the National Initiative for Cybersecurity Careers and Studies (NICCS) Portal.

DRAFT

INFORMATION TECHNOLOGY / CYBER SECURITY TRAINING
Module for Roles

Function Area: Operate and Maintain

Role Area: Data Administration

Roles:

- Data Security Analyst
- Data Management Systems Security
- Data Administrator
- Database Administrator
- Content Staging Specialist
- Data Architect
- Data Manager
- Data Warehouse Specialist
- Database Developer
- Information Dissemination Manager

Responsibility — Develop and administer databases and/or data management systems that allow for the storage, query, and utilization of data.

Knowledge Unit:

- Data Security
- Digital Forensics
- Database
- Cryptography and Encryption
- Architecture
- Identity Management / Privacy
- Information Systems
- Modeling and Simulation
- Incident Management

DRAFT

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Data Security	DS-2 DS-10 DS-18	DS-4	DS: 3 -8 DS: 13 - 14 DS: 16	DS: 3 - 6 DS-9 DS-12 DS: 17-18	DS-9 DS-11 DS-13 DS-15 DS: 17-18

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Digital Forensics				DF-6	DF-7 DF-31
Database		DB-5	DB-1 DB-2 DB-4 DB-6	DB-3 DB: 7 - 8 DB: 9 - 11	
Cryptography and Encryption		CR-10 CR-12	CR-1 CR-5	CR-3 CR-5 CR-7	CR-9
Architecture		ARCH-15	ARCH-2 ARCH-7 ARCH: 18 – 21	ARCH-1 ARCH-3 ARCH-4 ARCH-9	
Identity Management / Privacy	IM: 1-3 IM-7	IM-9 IM-11	IM-5	IM: 4-6 IM-9	IM-4 IM-5 IM-8 IM-10 IM-11
Information Systems	SI: 1-3 SI-10 SI: 27 -28 SI-30	SI-25	SI-4 SI-5 SI-9 SI-13 SI-25 SI-29	SI-5 SI-7 SI-8 SI-9 SI: 14 - 15 SI-20 SI-25 SI-29 SI-31	SI-17 SI-26 SI-31
Modeling and Simulation			MS: 2 – 3		
Incident Management	IR-20	IR-2 IR-3 IR-6 IR-14 IR-16 IR-18		IR-4 IR-12	IR: 2 - 3 IR-14

DRAFT

INFORMATION TECHNOLOGY / CYBER SECURITY TRAINING
Module for Roles

Function Area: Operate and Maintain

Role Area: Knowledge Management

Roles:

- Freedom of Information Act Official
- Information Owner
- Information Resource Manager
- Web Administrator
- Business Intelligence Manager
- Content Administrator
- Document Steward
- Information Manager

Responsibility — Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

Knowledge Unit:

- Information Systems
- Network and Telecommunications Security
- Emerging Technology
- Data Security
- IT Systems and Operations
- Incident Management

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Information Systems		SI-24	SI: 1-3 SI-22	SI: 1 - 4 SI: 7 - 8 SI-13 SI-22 SI-24	
Network and Telecommunications Security	NTS-22 NTS-23	NTS-9 NTS-44		NTS-9 NTS-34 NTS-44	
Emerging Technology	ET-1 ET-11	ET: 3 - 4 ET-6 ET-8 ET-10	ET-3 ET-5	ET: 3 - 5	

DRAFT

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Data Security		DS-2 DS-4 DS-18	DS-2 DS-5 DS: 7 - 8 DS-10 DS-13 DS-15	DS-2 DS: 4 - 5 DS: 7 - 10 DS-18	
IT Systems and Operations		ITOS-15 ITOS: 21 - 23	ITOS-4	ITOS-6 ITOS-8 ITOS-20 ITOS: 22 - 24 ITOS-27	ITOS-8
Incident Management	IR-20	IR: 1 - 2 IR-16			

DRAFT

INFORMATION TECHNOLOGY / CYBER
SECURITY TRAINING
Module for Roles

Function Area: Operate and Maintain

Role Area: Customer Service and Technical Support

Roles:

- Service Desk Representative
- Service Desk Operator
- Technical Support Personnel
- System Administrator
- Helpdesk Representative
- Customer Support Specialist
- Customer Support

Responsibility — Addresses problems, installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).

Knowledge Unit:

- Information Systems
- Incident Management
- Security Risk Management
- Systems and Applications Security
- Network and Telecommunications Security
- IT Systems and Operations

DRAFT

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Information Systems	SI: 1 - 3 SI: 5 – 7	SI-11 SI-18		SI: 8 - 16 SI: 18 - 19 SI-25 SI: 28 - 30	SI: 8 – 17 SI-19 SI-23 SI: 28 - 29
Incident Management	IR-1 IR-6 IR-16 IR-18 IR-20				
Security Risk Management	RM-3 RM: 5 - 6 RM-19	RM: 25 - 26 RM-28		RM: 20 - 23	

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Systems and Applications Security		SAS-8 SAS-20 SAS-22 SAS-25 SAS: 27 - 29		SAS: 1 - 2 SAS: 5 - 7 SAS: 29 - 30 SAS: 32 - 33	SAS-3 SAS-6 SAS: 9 - 10
Network and Telecommunications Security		NTS-9 NTS: 22 - 23 NTS: 27 - 28 NTS-35 NTS: 41 - 42		NTS: 1 - 6 NTS: 8 - 14 NTS: 16 - 21 NTS-25 NTS-35 NTS: 41 - 43 NTS-45 NTS-47 NTS-50	NTS: 3 - 4 NTS-6 NTS-17 NTS-51
IT Systems and Operations		ITOS: 3 - 4 ITOS-7		ITOS: 2 - 5 ITOS-7 ITOS: 10 - 11 ITOS-13 ITOS-20	

DRAFT

INFORMATION TECHNOLOGY / CYBER SECURITY TRAINING
Module for Roles

Function Area: Operate and Maintain

Role Area: Network Services

Roles:

- Network Administrator
- Telecommunication Personnel
- Network Security Specialist
- Telecommunication Engineer
- Continuous Monitoring Executer
- Cabling Technician
- Converged Network Engineer
- Network Analyst
- Network Designer
- Network Engineer
- Network Systems and Data Communications Analyst

Responsibility — Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

Knowledge Unit:

- Architecture
- IT Systems and Operations
- Information Assurance
- Information Systems
- Network and Telecommunications Security
- Security Risk Management
- Systems and Applications Security
- Cryptography and Encryption
- Data Security
- Configuration Management
- Computer Network Defense
- Web Technology
- Identity Management / Privacy
- Incident Management

DRAFT

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Architecture	ARCH: 10 - 12 ARCH-15 ARCH: 18 - 19	ARCH-5 ARCH-8	ARCH: 1 - 3 ARCH: 5 - 9 ARCH: 13 -14 ARCH-21	ARCH: 1 - 9 ARCH: 13- 14 ARCH: 16 - 17 ARCH-20	ARCH: 1 - 3 ARCH: 8 - 9 ARCH-14 ARCH-17 ARCH: 20 - 21
IT Systems and Operations	ITOS-4 ITOS-7 ITOS-11 ITOS-18 ITOS-23 ITOS-25	ITOS: 15 - 16 ITOS-27	ITOS: 1 - 2 ITOS-10 ITOS: 13 - 14 ITOS-16 ITOS-22	ITOS: 1 - 3 ITOS: 5 - 6 ITOS: 8 - 10 ITOS: 12 - 17 ITOS: 19 - 22 ITOS-24 ITOS: 26 - 27	ITOS-3 ITOS-6 ITOS-8 ITOS-10 ITOS: 14 - 15 ITOS-17 ITOS: 20 - 21 ITOS: 26 - 27
Information Assurance	IA-9	IA: 1 - 5	IA-3 IA: 6 - 7	IA: 6 - 8	IA: 1 - 2 IA-4 IA: 7 - 8
Information Systems	SI: 2 - 3 SI: 5 - 6 SI-16 SI-28	SI-7 SI-21 SI: 26 - 27 SI-30	SI-1 SI-4 SI: 9 – 12 SI-18 SI: 20 - 22 SI-25 SI-27 SI-29 SI-31	SI-1 SI: 7 - 15 SI: 18 - 20 SI: 22 - 25 SI-27 SI-29 SI: 30-31	SI-11 SI-13 SI-15 SI: 17 - 18 SI-23 SI: 26 - 27 SI: 29 - 31
Network and Telecommunications	NTS: 7 - 9 NTS: 11 - 16 NTS: 20 - 23 NTS-25 NTS: 34 - 36 NTS: 41 - 45 NTS-47 NTS-50	NTS-24 NTS: 27 - 28 NTS-30 NTS-33 NTS: 38 - 39 NTS-52	NTS-1 NTS-26 NTS-46 NTS-48 NTS-52	NTS: 1 - 6 NTS-10 NTS: 17 – 19 NTS: 27 - 33 NTS-38 NTS-40 NTS: 48 - 49	NTS: 3 - 6 NTS-10 NTS-17 NTS-24 NTS: 27 - 28 NTS: 30- 33 NTS-37 NTS: 39-40 NTS-51
Security Risk Management	RM-6	RM: 25 - 26 RM-28 RM: 30-31	RM: 7 - 8 RM-18	RM: 1 - 2 RM-10 RM-12 RM-14 RM-16 RM-18 RM-20 RM-22 RM: 33 - 34	RM: 1 - 2 RM-4 RM-7 RM: 9 - 10 RM: 12 - 14 RM-16 RM-18 RM-25 RM: 32 - 33
Cryptography and Encryption	CR-1 CR-3 CR-10	CR-10 CR-12 CR-14	CR-2 CR: 4 - 5 CR-12	CR: 4 - 5 CR: 11 - 12 CR-15	

DRAFT

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Data Security		DS-4 DS-18	DS-2	DS: 1 - 2 DS-4 DS-15 DS-18	
Configuration Management	CM-1 CM: 5 - 6 CM-9 CM-11	CM-7 CM-12 CM-15	CM-13	CM: 2 - 3 CM-8 CM-10 CM-12 CM-14	CM-4
Computer Network Defense	CND: 1 - 2 CND-11 CND: 17 - 20 CND-22	CND-4 CND: 9 -10 CND-12 CND: 14 - 16 CND: 29 - 30	CND-12	CND: 4 - 5 CND-8 CND: 14 - 16 CND-28	CND: 5 - 6 CND-10 CND-13 CND-21 CND: 24 - 29
Web Technology	WT-1			WT-9	
Identify Management / Privacy	IM: 1 - 3 IM-7			IM: 4 - 6	
Incident Management	IR: 1 - 3 IR-6 IR-16 IR-18 IR-20			IR: 9- 10 IR-12 IR-17	IR: 12 - 15

DRAFT

INFORMATION TECHNOLOGY / CYBER
SECURITY TRAINING
Module for Roles

Function Area: Operate and Maintain

Role Area: System Administration

Role:

- Directory Services Administrator
- System Administrator
- Operations Personnel / Management
- LAN administrator
- Platform Specialist
- Security Administrator
- Systems Operations Personnel
- Server Administrator
- Website Administrator

Responsibility — Installs, configures, troubleshoots and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control/ passwords/ account creation and administration.

Knowledge Unit:

- Information Systems
- Network and Telecommunications Security
- Architecture
- Security Risk Management
- Emerging Technologies
- Systems and Applications Security
- Digital Forensics
- Cryptography and Encryption
- Software
- Identity Management / Privacy
- Incident Management
- Configuration Management

DRAFT

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Information Systems	SI-3 SI-5 SI: 6 - 8 SI-10 SI-26 SI-28 SI-30	SI-10 SI-20 SI-25	SI: 1 - 2 SI-4 SI: 9 - 10 SI-16 SI-18 SI: 20 - 21	SI: 1 – 2 SI: 9 - 16 SI: 18 - 19 SI-23 SI-27 SI-29 SI-31	SI-1 SI: 11 – 13 SI: 15 - 17 SI-21 SI-23 SI-31
Network and Telecommunications Security	NTS-1 NTS-7 NTS-22 NTS-24 NTS-35 NTS-52	NTS-23 NTS-39		NTS-2 NTS: 4 - 5 NTS-23 NTS: 38 - 39	NTS: 2 - 6 NTS-23
Architecture	ARCH - 3 ARCH-14 ARCH-18	ARCH-2 ARCH-8 ARCH-13 ARCH-15	ARCH-1 ARCH: 4 - 6 ARCH-21	ARCH: 1 - 2 ARCH-4 ARCH-6	ARCH-21
Security Risk Management	RM-3 RM-5 RM-19 RM-21 RM-30	RM-2 RM: 25 - 28 RM-31	RM-8 RM-18	RM-1 RM-8 RM-18 RM-20 RM: 23 - 24 RM-34	RM-1 RM-7 RM: 22 - 23 RM-34
Emerging Technologies	ET: 1 – 2 ET: 8 - 11	ET-7		ET-4	
Systems and Applications Security	SAS: 1 – 3 SAS-8 SAS-11 SAS-20 SAS: 22 - 23 SAS: 29 - 30	SAS-25 SAS-27	SAS-4 SAS-24 SAS-26	SAS: 5 - 7 SAS-16 SAS: 25 - 26 SAS: 30 - 31	SAS-6 SAS: 9 - 10 SAS-16 SAS: 25 - 27 SAS: 30 - 31
Digital Forensics	DF-1	DF-6		DF: 6 – 7 DF-11	DF-7 DF-11
Cryptography and Encryption	CR-1 CR-5 CR-10 CR-12		CR-2	CR-11 CR-13	
Software	SW-9 SW-19 SW-21 SW-28 SW-30	SW-15	SW-7 SW-17 SW: 21 - 23 SW-29 SW-32	SW: 7 – 8 SW: 15 - 16 SW-18 SW: 22 - 23 SW-29	SW-8 SW-15 SW-22 SW-29
Identity Management/Privacy	IM-1 IM-3 IM-7 IM-9		IM-5	IM: 4 - 6 IM-8	IM-8 IM-11

DRAFT

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Incident Management	IR: 1- 3 IR-6 IR-11 IR-20			IR: 4 - 5 IR-9 IR-12	IR: 7 - 9
Configuration Management	CM: 1 – 2 CM: 5 – 6 CM-11	CM-7 CM: 9 - 10 CM-12 CM: 14 - 15		CM-3 CM: 8 - 10 CM: 14 - 15	CM-9

DRAFT

INFORMATION TECHNOLOGY / CYBER SECURITY TRAINING
Module for Roles

Function Area: Operate and Maintain

Role Area: Systems Security Analysis

Roles:

- Information technology / cyber security Officer
- Information Systems Security Officer
- Security Control Assessor
- Blue / Red Teams
- Penetration Tester
- Platform Specialist
- Security Administrator
- IA Operational Engineer
- Information technology / cyber security Analyst / Administrator / Manager

Responsibility — Conducts the integrations/testing, operations, and maintenance of systems security.

Knowledge Unit:

- Security Risk Management
- IT Security Awareness and Training
- Cryptography and Encryption
- Database
- IT Systems and Operations
- Architecture
- Information Assurance
- Information Systems
- Personnel Security
- Network and Telecommunication Security
- Identity Management / Privacy
- Configuration Management
- Software
- Systems and Applications Security
- Incident Management
- Procurement
- Compliance

DRAFT

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Security Risk Management	RM-3 RM: 5 - 6 RM-18 RM-33	RM: 25 - 31	RM-9 RM-17	RM: 1 - 2 RM-8 RM: 19 - 24 RM-29	RM: 1 – 2 RM-4 RM-7 RM: 9 – 16 RM: 21 - 22 RM: 32 RM-34
IT Security Awareness and Training		SAT-3 SAT: 5 - 6 SAT-8			SAT: 9 - 10
Cryptography and Encryption					CR: 1 - 5 CR-8 CR-10 CR-12
Database			DB-2	DB: 10 - 11	DB: 4 - 7
IT Systems and Operations	ITOS-7 ITOS: 10 -11	ITOS-16 ITOS-21 ITOS-23 ITOS-25 ITOS-27		ITOS: 12 - 13 ITOS-15 ITOS: 18 - 21 ITOS-24 ITOS-26	ITOS: 1 - 2 ITOS: 4 – 6 ITOS-8 ITOS: 17 - 19
Architecture	ARCH: 18 - 20	ARCH-2 ARCH-15			ARCH: 2 - 4 ARCH-17 ARCH-21
Information Systems		SI-26	SI-26	SI-27	SI: 17 - 18 SI- 22 SI: 27 - 28 SI: 30 - 31
Personnel Security		PS: 1 - 4 PS-8 PS: 10 - 12		PS-4 PS-11	PS: 8 - 9
Network and Telecommunication Security		NTS: 22 - 24 NTS: 27 - 28 NTS-31 NTS: 33 - 34 NTS-52		NTS-31 NTS-35 NTS-39 NTS-52	NTS-6 NTS: 8 - 9 NTS: 16 - 17 NTS: 20 - 26 NTS: 28 - 30 NTS: 33 - 34 NTS: 36 - 38 NTS: 40 - 47 NTS: 51 - 52
Identity Management/Privacy	IM: 7 - 8	IM-3 IM: 9 – 10		IM-5 IM-11	IM: 1 - 3 IM: 10 - 11
Information Assurance	IA: 1 – 2 IA-4	IA-5	IA-3 IA-6	IA-8	IA-7 IA-9
Configuration Management		CM-1 CM-7 CM-9 CM: 11 - 12		CM-2 CM-8 CM-10	CM-4
Software		SW: 28 - 29 SW-32		SW-29	SW: 24 - 28 SW: 30 – 32

DRAFT

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Systems and Applications Security	SAS-4	SAS-20 SAS-25 SAS-34		SAS-30 SAS-33	SAS-2 SAS-10 SAS-12 SAS-14 SAS: 15 - 24 SAS: 26 - 29 SAS-32 SAS-34
Incident Management	IR-18	IR: 1 - 3 IR-6 IR-13 IR-16 IR-20		IR: 2 - 3 IR: 11-12 IR-19	IR-1 IR-3 IR-5 IR: 7 - 10 IR: 13 - 17 IR: 19 - 20
Procurement		PROC: 5 - 8			
Compliance		COMP: 1 - 10			COMP-8

DRAFT

INFORMATION TECHNOLOGY / CYBER
SECURITY TRAINING
Module for Roles

Function Area: Securely Provision / Development

Role Area: Information Assurance Compliance

Roles:

- Accreditor
- Auditor
- Authorizing Official Designated Representative
- Certification Agent
- Certifying Official
- Designated Accrediting Authority
- Compliance Officer / Manager
- Compliance Analyst / Manager
- IA Manager
- IA Officer
- Portfolio Manger
- Risk / Vulnerability Manager
- Security Control Assessor
- Validator
- Inspector General
- Inspector / Investigator
- Regulatory Affairs Analyst
- IT Security Program Manager
- Governance Manager

Responsibility — Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new IT systems meet the organization's IA requirements. Ensures compliance from internal and external perspectives.

Knowledge Unit:

- Computer Network Defense
- Information Systems
- Network and Telecommunications Security
- Information Assurance
- Systems and Applications Security
- Emerging Technology
- Architecture
- Security Risk Management
- Incident Management
- Identity Management / Privacy

DRAFT

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
CND	CND-1 CND-4 CND-11 CND-15 CND-20 CND-22	CND-9 CND: 17 - 18 CND-29 CND-30	CND-3 CND-12 CND-14 CND-16	CND-2 CND-5 CND-8 CND: 13 - 14 CND-16 CND-19 CND-23 CND-29	CND-2 CND: 5 - 7 CND-10 CND-13 CND-15 CND-17 CND-19 CND-21 CND: 24 - 29
Information Systems	SI-3 SI: 5 - 8 SI-10 SI-26 SI-28 SI-30	SI-10 SI-20 SI-25	SI: 1 - 2 SI-4 SI: 9 - 10 SI-16 SI-18 SI: 20 - 21	SI : 1 - 2 SI: 9 - 16 SI: 18 - 19 SI-23 SI-27 SI-29 SI-31	SI-1 SI:11 - 13 SI: 15 - 17 SI-21 SI-23 SI-31
Network and Telecomm Security	NTS-7 NTS-11 NTS: 14-15 NTS:21-22 NTS-24 NTS-31	NTS-9 NTS-16 NTS-23 NTS-28 NTS-35 NTS:38-39 NTS-52		NTS-26 NTS-29 NTS-32 NTS-52	NTS-8 NTS: 11 - 12 NTS: 16 - 17 NTS-19 NTS-23 NTS: 27 - 29 NTS-32 NTS: 37 - 40 NTS: 51 - 52
Information Assurance	IA-1	IA: 2 - 5 IA-9	IA-3 IA-6	IA: 7 - 8	IA-2 IA: 7 - 9
Sys and App Security		SAS-10 SAS-12 SAS: 17 - 18 SAS-20 SAS: 25 - 27		SAS: 14 - 16	SAS-6 SAS: 9 - 10 SAS-12 SAS: 14 - 19 SAS-23 SAS: 26 - 27
Emerging Technology	ET-1	ET: 7 - 10	ET-9	ET-11	ET-6 ET: 8 - 10
Architecture	ARCH-15 ARCH-18			ARCH-3	ARCH-17 ARCH-21
Security Risk Management	RM: 5 - 6 RM-25 RM-30	RM: 26 - 28 RM-31	RM-8 RM-9	RM-4 RM-12 RM-14 RM-19	RM: 1 - 2 RM-7 RM: 10 - 11 RM-13 RM: 15 - 16 RM-18 RM-24 RM: 32 - 34

DRAFT

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Identity Management / Privacy	IM: 1 - 2 IM-7	IM-3 IM: 8 - 10		IM-5	IM-11
Incident Management	IR: 2 - 3 IR-20	IR: 6 - 7 IR-11 IR: 14 - 16 IR-18		IR-9 IR-10 IR-12 IR-14 IR-19	IR-5 IR-8 IR-11 IR: 13 - 17

DRAFT

INFORMATION TECHNOLOGY / CYBER SECURITY TRAINING
Module for Roles

Function Area: Securely Provision / Development

Role Area: Software Assurance and Software Engineering

Roles:

- Requirements Analyst
- Security Analyst
- Security Architect
- IA / Security Engineer
- Software Architect
- System Engineer
- Analyst Programmer
- Computer Programmer
- R&D Engineer
- Secure Software Engineer
- Reverse Engineer

Responsibility — Develops, creates, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

Knowledge Unit:

- Security Risk Management
- Data Security
- Systems and Applications Security
- Architecture
- Software
- Personnel Security
- Configuration Management
- Web Security
- Modeling and Simulation
- Identity Management / Privacy
- Information Systems
- Network and Telecommunications Security

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate

DRAFT

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Security Risk Management			RM-3 RM: 7 - 8 RM-19 RM-21	RM-22	
Data Security			DS: 3 - 10 DS: 12 - 14 DS-16 DS-18		
Systems and Applications Security		SAS-1 SAS-4 SAS-26	SAS-1 SAS-4 SAS-6 SAS-13 SAS-21 SAS-23 SAS-26 SAS-29 SAS-31 SAS-33		
Architecture			ARCH: 1 - 2 ARCH: 5 - 17 ARCH: 19 - 21	ARCH-1	
Software			SW: 1 - 32		
Personnel Security			PS-4 PS-11		
Configuration Management			CM: 2 - 6 CM-8 CM-11 CM: 13 - 14		
Web Security			WT-1 – 6		
Modeling and Simulation			MS: 2 - 3		
Identity Management / Privacy			IM: 1 – 6		
Information Systems			SI: 3 - 6 SI: 9 - 11 SI-13 SI-18 SI: 20 - 22		
Network and Telecommunications Security			NTS-2 NTS-7 NTS: 9: -10 NTS: 12 - 16		

DRAFT

INFORMATION TECHNOLOGY / CYBER SECURITY TRAINING
Module for Roles

Function Area: Securely Provision / Development

Role Area: Systems Security and Enterprise Architecture

Roles:

- Enterprise Security Architect
- IA / Security Architect
- Principal Security Architect
- Information System Security Engineer
- Network Security Analyst
- Security Solutions Architect
- Systems Security Analyst
- Ethical Hacker

Responsibility — Develops system concepts and works on the capabilities phases of the systems development lifecycle translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

Knowledge Unit:

- Identity Management / Privacy
- Architecture
- Cryptography and Encryption
- Database
- Information Assurance
- Information Systems
- Personnel Security
- Network and Telecommunications Security
- IT Systems and Operations
- Security Risk Management
- Configuration Management
- Software
- Systems and Applications Security
- Emerging Technologies
- Modeling and Simulation

DRAFT

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Identity Management / Privacy		IM-7		IM-1 – 5 IM: 8 - 9	
Architecture		ARCH-15	ARCH-5	ARCH: 5 - 6 ARCH-9 ARCH: 11 - 12 ARCH: 14 - 17	
Cryptography and Encryption				CR-1 CR: 3 - 5 CR: 9 - 12	
Database				DB-4 DB-7	
Information Assurance		IA-2 IA-4 IA-7	IA-8	IA-4 IA: 6 - 7	
Information Systems			SI: 3 - 7 SI-10 SI-12 SI-16 SI-18 SI: 20 - 21 SI: 26 – 28	SI: 1 - 3	
Personnel Security			PS-1 PS-4	PS-11	
Network and Telecommunications Security			NTS: 7 - 9 NTS: 11 - 12 NTS: 14 - 16 NTS: 23 - 24 NTS: 30 - 31 NTS: 35 - 36 NTS-42	NTS-16 NTS-23	
IT Systems and Operations			ITOS-4 ITOS-14 ITOS-23		
Security Risk Management			RM-4 RM: 6 - 7 RM-9 RM-26	RM-7 RM-26	
Configuration Management			CM-5 CM-9 CM-11 CM-13	CM-2 CM-5 CM-9 CM-11	
Software			SW: 11 - 12		

DRAFT

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Systems and Applications Security			SAS: 1 - 2 SAS-4 SAS-6 SAS-8 SAS-11 SAS-16 SAS-21 SAS: 22 - 23		
Emerging Technologies			ET-1 ET: 5 - 6 ET-8 ET: 10 – 11	ET-7 ET: 9 - 10	
Modeling and Simulation			MS: 1 – 3		

DRAFT

INFORMATION TECHNOLOGY / CYBER SECURITY TRAINING

Module for Roles

Function Area: Securely Provision / Development

Role Area: Technology Research and Development

Roles:

- R&D Engineer
- Capabilities and Development Specialist
- Applications Security Officer
- Cloud Provider

Responsibility — Conducts technology assessment and integration processes provides and supports a prototype capability and evaluates its utility.

Knowledge Units:

- Digital Forensics
- Software
- Compliance
- Cryptography and Encryption
- IT Systems and Operations
- Information Systems
- Network and Telecommunications Security
- Architecture
- Modeling and Simulation
- Information Systems
- Physical and Environmental Security
- Procurement
- Security Risk Management
- Systems and Applications Security
- Emerging Technologies

DRAFT

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Digital Forensics				DF: 3 - 4 DF-6 DF: 10 - 11 DF: 14 - 15 DF: 19 - 21 DF: 24 -25 DF: 27 - 29	

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Software			SW: 2 - 3 SW: 5 - 7 SW: 11 - 12 SW: 14 - 24 SW- 30 – 32		
Compliance				COMP: 1 - 7 COMP-10	
Cryptography and Encryption				CR: 1 – 11 CR: 13 - 15	
IT Systems and Operations				ITOS: 1 – 2 ITOS-4 ITOS-7 ITOS: 9 - 11 ITOS: 13 - 15 ITOS-19 ITOS: 22 - 23	
Information Systems				SI:1 – 3 SI-5-7 SI-9-12 SI-16 SI-21 SI-26 SI-28	
Network and Telecommunications Security				NTS-7 NTS: 9 - 10 NTS-12 NTS-15 NTS-21 NTS: 23 - 24 NTS-26 NTS-30 NTS-34 NTS-36 NTS: 45 - 46 NTS-52	
Architecture				ARCH: 1 - 3 ARCH: 5 – 15	
Modeling and Simulation				MS-1-3	
Information Systems				SI-5-7 SI-10 SI-21	
Physical and Environmental Security				PES-1 PES-6 PES-8	
Procurement		PROC-6 PROC: 8 - 9		PROC: 1 - 3	
Security Risk Management				RM-3 RM: 5 - 6 RM-8	

DRAFT

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Systems and Applications Security				SAS: 1 – 3 SAS: 10 - 11 SAS-24 SAS-26 SAS-30 SAS-34	
Emerging Technologies				ET: 1 - 11	

DRAFT

INFORMATION TECHNOLOGY / CYBER
SECURITY TRAINING
Module for Roles

Function Area: Securely Provision / Development

Role Area: Systems Requirements Planning

Roles:

- Business Analyst
- Business Process Analyst
- Computer Systems Analyst
- Contracting Officer
- Contracting Officer Technical Representative (COTR)
- Human Factors Engineer
- Requirements Analyst
- Solutions Architect
- System Consultant
- Systems Engineer

Responsibility — Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.

Knowledge Units:

- IT Systems and Operations
- Procurement
- Compliance
- Cryptography and Encryption
- Architecture
- Identity Management / Privacy
- Incident Management
- Information Assurance
- Information Systems
- Network and Telecommunications Security
- Architecture
- Security Risk Management
- Modeling and Simulation
- Information Systems
- Personnel Security
- Procurement
- Software
- Systems and Applications Security
- Emerging Technology

DRAFT

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
IT Systems and Operations		ITOS-16		ITOS: 8 - 10 ITOS: 15 - 16	
Procurement		PROC: 1 - 12		PROC: 1 – 5	
Compliance		COMP: 1 – 7 COMP: 9 - 10			
Cryptography and Encryption				CR: 1 – 5 CR: 14 - 15	
Architecture		ARCH 15 ARCH-18	ARCH 1 – 21		
Identify Management / Privacy		IM 1 – 3 IM-7 IM-9	IM 1 – 3 IM -7 IM-9		
Incident Management		IR-6		IR-10	
Information Assurance		IA: 1 – 5		IA: 6 – 8	
Information Systems		SI: 1 – 3	SI: 1 – 7 S:I 9 – 10 SI-16 SI-18 SI: 20 – 22 SI: 24 – 26		
Network and Telecommunication Security			NTS-1 NTS-7 NTS-13 NTS-15 NTS-23 NTS-25		
Architecture		ARCH- 15 ARCH-18 ARCH-21	ARCH 1 – 21	ARCH 1 - 21	
Security Risk Management		RM-3 RM-6 RM-30	RM-7 RM: 8 - 9	RM: 2 - 3 RM-8	
Modeling and Simulation			MS 1 – 3		
Information Systems			SI: 2 - 3 SI: 12 - 13 SI: 20 - 22		
Personnel Security			PS-1 PS-4		
Procurement		PROC 1 – 12			
Software		SW-14	SW-5		
Systems and Applications Security		SAS-22 SAS-26 SAS-34 SAS-28	SAS: 1 -3 SAS-26	SAS-6 SAS-23 SAS-26	

DRAFT

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Emerging Technology		ET: 1 – 4 ET: 8 – 11	ET: 1- 5	ET: 5 – 7	

DRAFT

INFORMATION TECHNOLOGY / CYBER SECURITY TRAINING

Module for Roles

Function Area: Securely Provision / Development

Role Area: Test and Evaluation

Roles:

- Application Security Tester
- Quality Assurance Tester
- Testing and Evaluation Specialist
- Systems Engineer
- R&D Engineer
- Information Systems Security Engineer
- Ethical Hacker
- Penetration Tester

Responsibility — Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying and validating of technical, functional and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.

Knowledge Units:

- Software
- IT Systems and Operations
- Information Assurance
- Information Systems
- Network and Telecommunications Security
- Architecture
- Information Systems
- Security Risk Management
- Identity Management / Privacy
- Systems and Applications Security

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Software		SW-14 SW: 28 - 29 SW-32		SW-3 SW-5	SW-1 SW-14 SW: 22 - 23 SW: 24 - 26 SW-28 - 32

DRAFT

Knowledge Unit	All	Manage	Design	Implement	Evaluate
IT Systems and Operations		ITOS- 23 ITOS-25 ITOS-27			ITOS: 4 - 5 ITOS: 7 - 8 ITOS-10 – 15 ITOS-18
Information Assurance		IA: 1 – 5			IA: 1 – 9
Information Systems		SI: 26 -28			SI: 5 – 7 SI: 16 – 18 SI: 26 - 31
Network and Telecommunications Security					NTS: 5 - 6 NTS: 8 - 16 NTS: 18– 40 NTS-52
Architecture		ARCH-15 ARCH-18		ARCH-17	ARCH-3-5 ARCH-10 – 12 ARCH: 17 - 18
Information Systems					SI-17 SI: 26 – 31
Security Risk Management		RM 26 – 32			RM: 1 - 34
Identity Management / Privacy		IR-6			IM-1 – 3 IR-5 IR-7 IR-10
Systems and Applications Security					SAS 1 – 2 SAS: 9-10 SAS-12 SAS: 14 - 26 SAS-29 SAS-30 SAS-32

DRAFT

INFORMATION TECHNOLOGY / CYBER SECURITY TRAINING

Module for Roles

Function Area: Securely Provision / Development

Role Area: Systems Development

Roles:

- IA Developer
- Program Developer
- Systems Engineer
- Information Systems Security Developer
- Security Engineer
- IA Engineer
- Configuration Manager

Responsibility — Works on the development phases of the systems development lifecycle.

Knowledge Units:

- Software
- IT Systems and Operation
- Configuration Management
- Cryptography and Encryption
- Database
- Architecture
- Personnel Security
- Identity Management / Privacy
- Information Assurance
- Information Systems
- Network and Telecommunications Security
- Systems and Applications Security
- Security Risk Management
- Modeling and Simulation
- Procurement

DRAFT

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Software		SW-14 SW-32	SW 1 – 3 SW-5 – 11 SW-14 SW-18 – 24 SW-32		

Knowledge Unit	All	Manage	Design	Implement	Evaluate
IT Systems and Operations			ITOS-4		
Configuration Management		CM-7 CM: 12 - 13	CM: 3 - 6 CM-13		
Cryptography and Encryption			CR-1 – 5 CR:14 - 15		
Database		DB-5	DB-2 DB-4 DB-6		
Architecture		ARCH-15	ARCH 9 – 14 ARCH-18 ARCH-20		
Personnel Security		PS-1 PS: 3 - 4	PS-1 PS: 3 - 4		
Identity Management / Privacy		IM-7 IM-9	IM 1 – 3 IM-7		
Information Assurance		IA-1	IA: 2 - 4 IA: 6 - 7		
Information Systems			SI: 4 – 7 SI-13 SI-16		
Network and Telecommunications Security		NTS-34	NTS 23 – 24 NTS-26 NTS: 34 -35 NTS: 40 – 47		
Systems and Applications Security			SAS-2 SAS-20 SAS-24 SAS-26 SAS-30		
Security Risk Management		RM-26 RM-28 RM: 30 - 31	RM-3 RM: 5 – 8		
Modeling and Simulation			MS-3		
Procurement		PROC-1 – 5			

DRAFT

INFORMATION TECHNOLOGY / CYBER SECURITY TRAINING
Module for Roles

Function Area: Securely Provision / Defend

Role Area: Computer Network Defense Analysis

Roles:

- CND Security Personnel
- System Administrator
- Network Security Administrator
- Network Security Specialist
- CND Analyst
- Cryptographer
- CND Auditor
- Security Analyst
- Cyber Security Intelligence Analyst
- Focused Operations Analyst
- Incident Analyst
- Network Defense Technician
- Security Operator
- Sensor Analyst

Responsibility — Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

Knowledge Units:

- Digital Forensics
- Software
- Computer Network Defense
- Configuration Management
- Compliance
- Cryptography and Encryption
- Data Security
- Incident Management / Privacy
- Information Systems
- Network and Telecommunications Security
- Architecture
- Emerging Technology
- Security Risk Management

DRAFT

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Digital Forensics				DF-7 DF-10 DF: 22 – 26	
Software				SW-4 SW: 16 – 17 SW-30 – 32	
Computer Network Defense		CND 9 – 12 CND 15 – 20 CND 22 – 24 CND-29		CND 1 - 30	
Configuration Management				CM 2 - 7	
Compliance		COMP 1 – 7		COMP 1 COMP-2 COMP 4 – 6 COMP-10	
Cryptography and Encryption				CR-12	
Data Security				DS: 11 - 12	
Incident Management / Privacy		IM 1 – 3		IM 1 – 5	
Information Systems				SI-15 SI-26 SI 28 – 31	
Network and Telecommunications Security		NTS – 23 NTS-52		NTS 1 – 6 NTS-9 – 11 NTS-16 – 18 NTS 23 – 26 NTS-29 – 34 NTS 38 – 39 NTS 52	
Architecture		ARCH 15 - 16		ARCH 7 – 9 ARCH 15 – 16	
Emerging Technology		IR 16 - 20		IR-12 – 20	
Security Risk Management		RM 26 - 33		RM 1 – 6 RM-10 RM-12 – 16 RM 18 – 19 RM 22 -24 RM-34	

DRAFT

INFORMATION TECHNOLOGY / CYBER SECURITY TRAINING
Module for Roles

Function Area: Defend

Role Area: Incident Response and Handling

Roles:

- Incident Response Personnel
- Digital Forensics Specialist
- System Administrator
- Network Administrators
- Business Contingency Planner
- IT Contingency Planner
- Damage Assessment Teams
- Information Systems Security Officer
- Computer Crime Investigator
- Incident Handler
- Incident Responder
- Intrusion Analyst

Responsibility — Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses planning, mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information technology / cyber security. Investigates and analyzes all relevant response activities.

Knowledge Units:

- Digital Forensics
- Computer Network Defense
- Incident Management
- Information Assurance
- Information Systems
- Network and Telecommunications Security
- Architecture
- Security Risk Management

DRAFT

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Digital Forensics	DF-1 DF-4	DF-6 DF: 9 - 10 DF: 23 - 26	DF-3 DF-27	DF-2 DF: 6 - 7 DF-9 DF-11 DF-13 DF-15 DF: 19 - 21 DF: 27 - 29	DF-2 DF: 5 - 9 DF: 11 - 18 DF: 20 - 24 DF: 28 - 31
Computer Network Defense	CND-1 CND-11 CND-12 CND-18 CND-20	CND-9 CND-15 CND-29 CND-30	CND-2 CND-17	CND-2 CND-4 CND-6 CND-8 CND: 13 - 14 CND: 16 - 17 CND-19 CND-22 CND-28	CND: 2 - 8 CND-10 CND-13 CND: 16 - 17 CND-19 CND: 21 - 28
Incident Management	IR-1 IR-2 IR-20	IR-3 IR-6 IR-11 IR: 15 - 16 IR: 18 - 19		IR: 3 - 7 IR-10 IR: 12 - 19	IR-3 IR: 5 - 11 IR: 13 - 15
Information Assurance	IA-4	IA: 1 - 2 IA-5	IA-3 IA-6	IA: 6 - 9	IA-1 IA-7
Information Systems	SI: 5 - 7	SI: 26 - 27 SI-30	SI-4 SI-16 SI-18	SI-4 SI: 11 - 12 SI: 16 - 19 SI-24 SI-26 SI: 28 - 29 SI-31	SI: 12 - 13 SI-15 SI-19 SI-23 SI: 26 - 28 SI-30
Network and Telecommunications Security	NTS: 15 – 16 NTS: 22 - 24 NTS: 34 - 35 NTS: 42 - 43	NTS-7 NTS-9 NTS-27 NTS-36 NTS: 38 - 39	NTS: 12 - 14 NTS-21 NTS-26 NTS: 30 – 31 NTS-31 NTS-41 NTS-44 NTS-47	NTS: 1 - 2 NTS: 5 - 11 NTS: 13 - 14 NTS-18 NTS: 20 – 21 NTS: 25 – 26 NTS: 28 - 33 NTS-37 NTS-39 NTS-44 NTS-52	NTS: 3 - 6 NTS-9 NTS-11 NTS-14 NTS: 17 - 20 NTS-25 NTS: 27 – 28 NTS-33 NTS-37 NTS: 39 - 40 NTS-44 NTS-52
Architecture	ARCH-18		ARCH-5 ARCH-17	ARCH-3 ARCH-7 ARCH-13 ARCH-17	ARCH: 2 - 3 ARCH-13 ARCH-17 ARCH-21

DRAFT

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Security Risk Management	RM: 5 - 6	RM: 25 - 26 RM-28 RM: 30 - 31	RM-8	RM-2 RM: 7 - 8 RM-10 RM-12 RM: 14 - 16 RM-19 RM: 21 - 22	RM: 1 - 4 RM-7 RM-9 RM: 11 - 18 RM-24 RM: 32 - 34

DRAFT

INFORMATION TECHNOLOGY / CYBER SECURITY TRAINING
Module for Roles

Function Area: Defend

Role Area: Computer Network Defense Infrastructure Support

Roles:

- Network Security Personnel
- Enterprise Architect
- Information Systems Security Engineer
- IDS / IPS specialist
- Information Systems Security Engineer
- IDS Administrator
- IDS Engineer
- IDS Technician
- Network Security Engineer
- Security Specialist

Responsibility — Tests, implements, deploys, maintains, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.

Knowledge Units:

- Digital Forensics
- Computer Network Defense
- Cryptography and Encryption
- Identity Management / Privacy
- Incident Management
- Information Assurance
- Information Systems
- Network and Telecommunications Security
- Architecture
- Security Risk Management
- Web Security

DRAFT

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Digital Forensics		DF 25 – 31		DF 1 – 4 DF-6 DF 25 - 31	
Computer Network Defense		CND 1 – 30		CND 1 - 30	
Cryptography and Encryption		CR 1 - 5		CR 1 – 8 CR 1- 15	
Identity Management / Privacy		IM 1 – 3 IM 9 - 11		IM 1 - 11	
Incident Management		IR 1 – 20		IR 1 - 20	
Information Assurance		IA 1 - 9		IA 6 - 8	
Information Systems				SI 26 - 31	
Network and Telecommunications Security		NTS 21 – 26		NTS 20 – 34 NTS 37 – 39	
Architecture				ARCH 17 – 18	
Security Risk Management		RM 25		RM 4 – 8 RM 10 - 16	
Web Security				WT 1 – 10	

DRAFT

INFORMATION TECHNOLOGY / CYBER SECURITY TRAINING

Module for Roles

Function Area: Protect

Role Area: Vulnerability Assessment and Management

Roles:

- Risk / Vulnerability Analysts
- Auditors
- Ethical Hacker
- Blue Team Technician
- Close Access Technician
- CND Auditor
- Compliance Manager
- Governance Manger
- Internal Enterprise Auditor
- Penetration Tester
- Red Team Technician
- Reverse Engineer
- Risk / Vulnerability Manger

Responsibility — Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

Knowledge Units:

- Digital Forensics
- Software
- Computer Network Defense
- Procurement
- Compliance
- Personnel Security
- Identity Management / Privacy
- Information Assurance
- Information Systems
- Network and Telecommunications Security
- Architecture
- Systems and Applications Security
- Security Risk Management

DRAFT

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Digital Forensics				DF 9 – 11	
Software		SW 28 – 30 SW- 32		SW 22 – 27 SW-31	
Computer Network Defense		CND-29 CND 16 - 20		CND-2 CND-4 CND-6 CND 8 – 13 CND 16 – 20 CND 22 – 30	
Procurement		PROC-3 PROC-9			
Compliance		COMP 1 - 10		COMP 1 - 10	
Personnel Security		PS-1 – 4 PS-11		PS-12	
Identity Management / Privacy		IM 1- 3		IM 1 – 5 IM 6 – 7	
Information Assurance		IA 1 - 5		IA 1 - 7	
Information Systems				SI-16 SI 26 - 31	
Network and Telecommunications Security		NTS-39		NTS-15 NTS 21 – 28 NTS 34 NTS-39	
Architecture				ARCH: 8 – 11 ARCH: 17 - 18	
Systems and Applications Security		SAS-2 SAS-10 SAS-12 SAS 14 - 24		SAS-2 SAS-10 SAS-12 SAS 14 - 24	
Security Risk Management		RM 1 – 34		RM 1 - 34	

DRAFT

INFORMATION TECHNOLOGY / CYBER SECURITY TRAINING
Module for Roles

Function Area: Respond / Investigate

Role Area: Investigation

Roles:

- Incident Response Team
- Computer Crime Specialist
- Special Agent
- Special Analyst

Responsibility — Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, analysis, interview and information gathering techniques. Processes appropriately balance the benefits of evidence gathering and safeguarding for prosecution.

Knowledge Units:

- Digital Forensics
- Compliance
- Physical and Environmental Security
- IT Systems and Operations
- Security Risk Management

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Digital Forensics		DF-21 DF 23 – 31		DF 1 - 31	DF 1 - 31
Compliance				COMP 1 – 7 COMP 9 COMP 10	
Physical and Environmental Security				PES-1 PES 4 – 6 PES-8	
Security Risk Management		RM-28 – 31		RM 1 – 7 RM 10 – 2 RM 24 – 28 RM 32 - 34	

DRAFT

INFORMATION TECHNOLOGY / CYBER SECURITY TRAINING
Module for Roles

Function Area: Respond / Investigate

Role Area: Digital Forensics

Roles:

- Certified Computer Examiner
- Digital Forensics Analyst
- Digital Forensics Engineer
- Digital Forensics Practitioner
- Digital Forensics Professional
- CND Forensic Analyst
- Forensics Analyst (cryptologic)
- Forensics Technician
- Digital Media Collector
- Digital Forensics Examiner
- Network Forensic Examiner

Responsibility — Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

Knowledge Units:

- Digital Forensics
- Software
- Computer Network Defense
- IT Systems and Operations
- Compliance
- Cryptography and Encryption
- Data Security
- Incident Management
- Information Assurance
- Information Systems
- Network and Telecommunications Security
- Architecture
- Security Risk Management
- Web Security

DRAFT

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Digital Forensics				DF 1 - 31	
Software				SW 22 – 27 SW-30	
Computer Network Defense				CND 1 – 4 CND 9 – 11 CND-13 CND 16 – 21 CND-26	
IT Systems and Operations				ITOS-5 ITOS-18 ITOS-21 ITOS-26	
Compliance				COMP 1 – 7 COMP 10	
Cryptography and Encryption				CR 1 – 10 CR-14 CR-15	
Data Security				DS-2 DS-15	
Incident Management				IR 1 – 20	
Information Assurance		IA 1 – 5		IA 1 – 5 IA-9	
Information Systems				SI 1 – 3 SI 5 – 7 SI 9 - 12	
Network and Telecommunications Security				NTS 22 – 34 NTS: 37 – 41	
Architecture				ARCH 16 – 21	
Security Risk Management				RM 1 – 6 RM 10 – 17	
Web Security				WT-6	

DRAFT

INFORMATION TECHNOLOGY / CYBER
SECURITY TRAINING
Module for Roles

Function Area: Oversight, Management and Development

Role Area: Legal Advice and Advocacy

Roles:

- Office of General Counsel Staff
- Legal Advisor / SJA
- Cyber Lawyer

Responsibility — Provide legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes and make a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.

Knowledge Units:

- Procurement
- Compliance
- Cryptography and Encryption
- Emerging Technologies
- Security Risk Management

DRAFT

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Procurement		PROC-6		PROC: 6 - 9	
Compliance				COMP: 1 - 5 COMP-10	
Cryptography and Encryption		CR-1		CR-1	
Emerging Technologies		ET-1		ET-1	
Security Risk Management		RM-30 RM-28 RM-24			

INFORMATION TECHNOLOGY / CYBER
SECURITY TRAINING
Module for Roles

Function Area: Oversight, Management and Support

Role Area: Strategic Planning and Policy Development

Roles:

- Policy Analyst
- Security Policy Manager
- Policy Writer / Strategist
- IT Function Management
- IT Director
- Operations Management
- Heads of Government
- National Manager
- Program Manager
- Chief Technology Officer
- Chief Information Officer
- Command Information Officer
- Information technology / cyber security Policy Analyst
- Information technology / cyber security Policy Manager

a) **Responsibility** — Applies knowledge of priorities to define an entity's direction, determine how to allocate resources, and identify program or infrastructure that are required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements.

Knowledge Units:

- Computer Network Defense
- Procurement
- Compliance
- Architecture
- Physical and Environmental Security
- Information Assurance
- Architecture
- Security Risk Management
- Emerging Technologies

DRAFT

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Computer Network Defense Security		CND-10 CND-15 CND-18 CND-29		CND-9 CND-12 CND-15	
Procurement		PROC-1		PROC: 1 - 5 PROC: 7 - 12	
Compliance		COMP: 3 - 5		COMP: 1 - 7 COMP: 9 – 10	
Architecture		ARCH-15		ARCH-5 ARCH: 15 - 16 ARCH-18	
Physical and Environmental Security		PES-1 PES-6 PES-8			
Information Assurance		IA 1 – 7		IA 1 - 7	
Architecture		ARCH-15 ARCH-18		ARCH-5 ARCH-8 ARCH-13 ARCH: 15 - 16 ARCH-18	
Security Risk Management		RM: 25 - 32		RM: 5 - 6 RM-25 – 32	
Emerging Technologies		ET: 9 - 10		ET: 1 - 2 ET: 6 - 11	

DRAFT

INFORMATION TECHNOLOGY / CYBER SECURITY TRAINING
Module for Roles

Function Area: Oversight, Management and Support

Role Area: Awareness, Education and Training

Roles:

- Security Trainers
- End Users / System Users
- Training Coordinators
- Cyber Trainer
- Information technology / cyber security Trainer
- Human Resource Personnel

Responsibility — Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, and evaluates training courses, methods, and techniques as appropriate.

Knowledge Units:

- IT Security Awareness and Training
- Personnel
- Management

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
IT Security Awareness and Training	SAT 1 – 12				
Personnel		PS 1 – 2 PS-5 PS-8 PS: 11-12			
Management		PM-9 PM-12 PM-53			

DRAFT

DRAFT

INFORMATION TECHNOLOGY / CYBER SECURITY TRAINING
Module for Roles

Function Area: Operate and Maintain

Role Area: Information Systems Security Operations

Roles:

- Cyber Security Officer
- Chief Information technology / cyber security Officer
- Enterprise Security Officer
- Information technology / cyber security Officer
- Senior Agency Information technology / cyber security Officer

Responsibility — Oversees the information assurance (IA) program of an information system in or outside the network environment may include procurement duties.

Knowledge Units:

- Procurement
- Compliance
- Architecture
- Incident Management
- Information Assurance
- Information Systems
- Network and Telecommunications Security
- Systems and Applications Security
- Security Risk Management
- Procurement
- Identity Management / Privacy
- Emerging Technologies

DRAFT

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Procurement		PROC 1 – 12			
Compliance		COMP: 3 - 7 COMP: 9 - 10		COMP 1 - 2 COMP-6 - 10	
Architecture				ARCH 1 – 3 ARCH 5 – 15 ARCH-18	

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Incident Management		IR 1 – 3 IR 6-7 IR 11 IR 16 - 20		IR 12 – 20	
Information Assurance		IA 1 – 5 IA-9		IA 1 – 9	
Information Systems		SI 26 - 30			
Network and Telecommunications Security		NTS 21 – 28 NTS 33- 35 NTS 38 – 39		NTS 30 - 31	
Systems and Applications Security		SAS 10 – 12 SAS-14 – 26 SAS 28 – 34			
Security Risk Management		RM 1 - 34		RM 1 – 34	
Procurement		PROC 7 – 12			
Identity Management / Privacy		IM 1 – 3 IM 7 - 11		IM 4 – 6 IM-7 IM-11	
Emerging Technologies		ET-1 ET-7 ET-9 – 11	ET-1		

DRAFT

INFORMATION TECHNOLOGY / CYBER SECURITY TRAINING
Module for Roles

Function Area: Oversight, Management and Development

Role Area: Security Program Management

Roles:

- Information Assurance Manager (IAM)
- Information Assurance Security Officer (IASO)
- Information technology / cyber security Officer (ISO)
- Information technology / cyber security Program Manager
- Information Systems Security Manager (ISSM)
- Information Systems Security Officer (ISSO)
- Security Program Director
- Risk Executive
- CISO / SAISO
- Common Control Provider
- It Function Management / IT Director
- End Users / Systems Users
- Cloud Providers
- Enterprise Security Officer
- Facility Security Officer
- Principle Security Architect
- Risk Executive
- Senior Agency Information technology / cyber security Officer

Responsibility: Concentrates on protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity and availability.

Manages information technology / cyber security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.

Knowledge Units:

- Digital Forensics
- Computer Network Defense
- Procurement
- Compliance
- Cryptography and Encryption
- Incident Management
- Information Assurance
- Information Systems
- Network and Telecommunications Security

DRAFT

- Architecture
- Security Risk Management

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Digital Forensics	DF-4 DF-10	DF-1 DF-6 DF 23 - 26	DF-3 DF-6 - 7 DF-25 - 26	DF-1 DF-3 DF-6	
Computer Network Defense	CND-15 CND 17 - 18	CND 11 - 12 CND-29	CND-1 CND-2 CND-4	CND-1 CND-2 CND-4 CND-12	CND-10
Procurement	PROC-1 PROC-11	PROC-2 PROC-4 PROC-6 PROC-8 PROC-12		PROC-9	
Compliance	COMP-10	COMP-1 COMP 3 – 5 COMP-7	COMP-6 COMP-9		COMP-2 COMP-5 COMP-8
Cryptography and Encryption		CR 1 - 5 CR-10 CR-12			
Incident Management		IR 1 - 3 IR-6 IR-11 IR-16 IR-18 IR-20			
Information Assurance		IA 1 - 7 IA-9			
Information Systems		SI-26 SI-28 SI-30			

DRAFT

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Network and Telecommunications		NTS-7 NTS-9 NTS 13 - 14 NTS 16 - 17 NTS-23 - 24 NTS-28 NTS-34 - 36 NTS-41 - 42			
Architecture		ARCH-5 ARCH 8 - 10 ARCH-12 - 15 ARCH-18			
Security Risk Management	RM-30 RM-31	RM-3 RM-5 - 6 RM 26 - 28			

DRAFT

INFORMATION TECHNOLOGY / CYBER
SECURITY TRAINING
Module for Roles

Function Area: Oversight, Management and Development

Role Area: Management

Roles:

- Senior Management
- Senior Systems Manger
- Program Manager
- Project Manager
- Functional Manager
- CISO

Responsibility — Manages information programs and the security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.

Knowledge Units:

- Management
- Compliance
- Procurement
- Identity Management / Privacy
- Information Assurance
- IT Security Awareness and Training
- Personnel Security
- Security Risk Management

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Management		PM 1 - 53			
Compliance	COMP-1 COMP 4 - 5	COMP-3 COMP-6 – 7 COMP 9 - 10		COMP-2 COMP 9 - 10	COMP-8
Procurement		PROC 1 - 4 PROC 6 - 9 PROC-11 - 12			PROC-2
Identity Management/ Privacy		IM 1 - 3 IM 7 - 11			

DRAFT

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Information Assurance		IA 1 -7 IA-9			
IT Security Awareness and Training		SAT-1 SAT-3 SAT 5 – 6 SAT 9 - 12			
Personnel Security		PS 1 - 4 PS 6 PS 8 – 12			
Security Risk Management		RM 3 - 6 RM-9 RM 18 – 20 RM 25 – 33			

DRAFT

INFORMATION TECHNOLOGY / CYBER
SECURITY TRAINING
Module for Roles

Function Area: Oversight, Management and Development

Role Area: Privacy

Roles:

- Chief Privacy Officer
- Privacy Act Officer / Official
- Privacy Information Professional
- Privacy Officer
- Senior Agency Official for Privacy
- Human Resources
- Health Care Officer
- Project / Program Manager

Responsibility: Developing and managing an organization's privacy compliance program. Establishes a risk management framework and governance model to assure the appropriate handling of Personally Identifiable Information (PII), and ensures that PII is managed throughout the information life cycle – from collection to disposal.

Knowledge Units:

- Compliance
- Identity Management / Privacy
- Incident Management
- IT Security Awareness and Training
- Management
- Personnel Security

DRAFT

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Compliance		COMP-2 COMP 4 - 7		COMP-2 COMP 4 - 5	COMP-8
Identity Management /Privacy		IM-1 IM-3 IM-7 IM-9		IM 1 - 5 IM 8 - 11	

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Incident Management		IR-1 IR-6 IR-16 IR-18 – 20		IR: 15 - 16	IR-17
IT Security Awareness and Training		SAT-1 SAT 3 - 4		SAT 11 - 12	
Management		PM-1 – 3 PM-8 PM-11 - 13 PM-15 PM-23 PM-26 PM-34 PM-46 PM-49 PM-51		PM-5 - 7	
Personnel Security		PS-3 PS-5 - 7 PS-1 – 12		PS-12	

DRAFT

INFORMATION TECHNOLOGY / CYBER
SECURITY TRAINING
Module for Roles

Function Area: Oversight, Management and Development

Role Area: Procurement

Roles:

- Procurement Officer
- Management
- Contracting Officers
- System Owner
- Program Manager
- Project Manager
- Budgeting Officer

Responsibility – Procures resources as needed. Develops and executes contracts to include security controls. Ensures deliverables are compliant with Federal and Organizational security control requirements.

Knowledge Units:

- Procurement
- Management
- Compliance

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Procurement	PROC 1 - 2	PROC 6 - 9 PROC-11 - 12		PROC-3 - 9	PROC-4 PROC-10
Management	PM-37	PM-1 - 4 PM-8 PM-10 PM-12 PM-14 PM-16 PM-22 - 23 PM-25 PM-32 - 33		PM-4 PM-6 - 8 PM-32 - 33	
Compliance		COMP-1 COMP-3 - 5 COMP-7		COMP-2 - 5	

DRAFT

INFORMATION TECHNOLOGY / CYBER SECURITY TRAINING
Module for Roles

Function Area: Oversight, Management and Development

Role Area: Personnel Security

Roles:

- Hiring Manager
- Human Resources Manager
- First Responders

Responsibility – Responsible for hiring, termination and training of the IA workforce. Ensures background checks are completed. Assists with implementing the need-to-know concept. Key player in the business contingency planning and execution.

Knowledge Units:

- Management
- Personnel Security
- Security Risk Management
- IT Security Awareness and Training
- Compliance
- Identity Management / Privacy
- Incident Management

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Management		PM 1 - 4 PM-6 - 8 PM-11 - 15 PM-17 PM-19 PM-23 PM-25 PM-34 - 36 PM-46 PM-48 - 51		PM: 7 - 8 PM-11	
Personnel Security		PS-1 - 12		PS-1 - 12	
Security Risk Management		RM-25 - 31			
IT Security Awareness and Training		SAT-3 SAT-6 SAT-10	SAT-1 - 3 SAT-5 - 7 SAT-9	SAT-4 SAT-8 SAT-1 – 12	
Compliance		COMP 1 - 7	COMP-8	COMP-1	

DRAFT

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Identity Management/ Privacy		IM-1 - 3 IM-7 - 11		IM-10	
Incident Management		IR-1 IR-6 IR-15 IR-20		IR-19	

DRAFT

INFORMATION TECHNOLOGY / CYBER
SECURITY TRAINING
Module for Roles

Function Area: Oversight, Management and Development

Role Area: Physical and Environmental Security

Roles:

- Facility Security Officer
- Physical Security Administrator
- Physical Security Officer
- First Responders
- Physical Security Professional

Responsibility – Ensures implementation and maintenance of physical security controls both in buildings hosting personnel as well as datacenters. Key player in contingency planning activities.

Knowledge Units:

- Compliance
- Enterprise Continuity
- Incident Management
- Industrial Controls Systems
- Physical and Environmental Security
- Security Risk Management

Corresponding Knowledge and Skills

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Compliance		COMP-3 -5 COMP-7 COMP-9			COMP-8
Enterprise Continuity		ECP: 1 - 2 ECP: 5 -6 ECP-9 ECP: 14 – 16	ECP-3 ECP-7 - 8	ECP: 1 -2 ECP-5 ECP: 14 - 18	ECP: 1 - 2 ECP-4 ECP-7 ECP: 10 - 13
Incident Management		IR: 1 - 3 IR-6 IR-12 IR-20		IR-12 IR-14 IR-19	IR-15
Industrial Controls Systems		ICS: 1 – 2		ICS: 2 - 7	

DRAFT

Knowledge Unit	All	Manage	Design	Implement	Evaluate
Physical and Environmental Security		PES-1 PES-6 PES-8		PES: 1 - 9	
Security Risk Management		RM: 25 - 28 RM: 30 – 31	RM-8	RM-29 RM-30	RM-9 RM: 25 - 26

DRAFT

Appendix D: Sample Evaluation Forms

Evaluation Objectives				
Levels of Evaluation Student	**Level 1: Satisfaction**	**Level 2: Learning Effectiveness**	**Level 3: Performance Effectiveness**	**Level 4: Training Program Effectiveness**
Type of Training CyberSecurity	How well did the student think he/she grasped the security concepts? For CBT, how many attempts did it take for the student to pass the test?	How did the majority of students perform on the test, (e.g., do aggregated post-test answers show sufficient improvement over pre-test answers)?	How well is the student using the core skill set in his or her daily activities routine?	Did the number and severity of security incidents go down as a result? Did the cost of security compliance go down? If so, how much?
Training	How well did the training program fit the student's expectations?	Did the training program demonstrably and sufficiently increase the scope and/or depth of the student's skill set?	How well is the student applying the new security skills to functional job requirements?	Did the number and severity of security incidents go down as a result? Did the cost of security compliance go down? If so, how much?
Education	Did the course of study advance the student's career development or professional qualifications in information technology / cyber security?	Could the student apply the increased knowledge to a real world situation adequately?	How well is the student's acquired information technology / cyber security knowledge being used to advance agency goals & objectives?	Did the number and severity of security incidents go down as a result? Did the cost of security compliance go down? If so, how much?

Exhibit D-1 Evaluation Objectives

DRAFT

Sample Questionnaire — Level 1 Evaluation Training Assessment by Student

1. Indicate your highest level of education:

   High School graduate or less
   Some college/technical school
   Associate degree or technical certification
   Bachelor's Degree
   Master's Degree
   Doctorate

2. Indicate the total number of courses you have completed in subject areas related to this training:

   0 1-4 5-10 11-15 More than 15

3. Indicate how long it has been since you took a course in the subject area of this training:

   This is my first course in this subject
   Less than 1 year
   1-3 years
   4-6 years
   More than 6 years

4. Indicate the extent of your work experience in the general subject areas of this training:

   None
   Less than 1 year
   1-3 years
   4-6 years
   More than 6 years

5. For my preparation and level of knowledge, the training was:

   Too elementary
   Somewhat elementary
   Somewhat difficult
   Too difficult
   About right

6. The pace at which the subject matter was covered was:

   Too slow
   Somewhat slow
   Somewhat fast
   Too fast
   About right

7. For what I got out of this training, the workload was:

   Light
   About right
   Heavy

8. Considering my previous experience with this subject matter, the course content was:

   Out of date
   Somewhat current
   Current

9. Which of the following best describes the usefulness of this training for your job:

DRAFT

Not particularly useful Very useful
Somewhat useful Essential

10. How much did you learn from this training:
Not much A moderate amount
A great deal

Please send any suggestions to:

Student Perception of Instructor

Extent to which the instructor successfully:	**Excellent**	**Good**	**Fair**	**Poor**	**N/A**	**Comments**
1. Presented material in an organized manner						
2. Communicated knowledge of the subject matter						
3. Made difficult concepts understandable						
4. Used class time effectively						
5. Stimulated interest in the subject area						
6. Demonstrated positive attitude toward participants						
7. Overall, I would rate this instructor						

Student Perception of Course Quality

Course content:	**Excellent**	**Good**	**Fair**	**Poor**	**N/A**	**Comments**
1. Clarity of course objectives						
2. Agreement between course objectives and course content						

DRAFT

3. Agreement between Tests/Exams and course objectives						
4. Degree to which the organization of the course enhanced my						
5. Opportunities to practice/apply course content during						
6. Effectiveness of textbook(s), handouts, or other material						
7. Quality of classroom/lab facilities						
8. Overall, I would rate this course						

Exhibit C-2 Sample Questionnaire — Level 1 Evaluation Training Assessment by Student

DRAFT

Sample Questionnaire — Level 3 Evaluation Training Assessment by Supervisor

SECTION I - COURSE RELATION TO JOB REQUIREMENTS

1. What was the chief reason for nominating the employee for this course?
   Information is required in present job
   Information is required in new job
   Course provides prerequisite or background for other training
   Course is required to meet certification
   Course provides general career development
   Other (please specify)

2. Considering past experience/training and present/future job assignments, how well timed was this course in the employee's career?
   Took before needed
   Took when needed
   Needed course earlier, but wasn't offered
   Needed course earlier, but couldn't get in
   Didn't need course and probably will never use it
   Unable to assess at this time

3. Which of the following best describes the usefulness of this training for the employee's job?
   Essential
   Very useful
   Somewhat useful
   Not particularly useful
   Unable to assess at this time

4. How frequently does the employee need the skills or knowledge acquired in this course?
   Daily
   Weekly
   Periodically
   Not currently used, but needed for background or future use
   Criteria does not apply to this course

SECTION II - COURSE IMPACT ON EMPLOYEE PERFORMANCE

Rate the degree to which the employee's information-related job performance was affected by the training in this course.

Job Impact	**1**	**2**	**3**	**4**	**5**
Knowledge of information technology / cyber security- related job duties					

DRAFT

Technical skills (include applicable language-related skills)					
Productivity					
Accuracy					
Use of job aids (e.g., reference aids, software applications)					

Overall work quality:

Legend:
1 = Greatly improved 3 = Moderately improved 5 = Not applicable
2 = First-time impact 4 = No change

SECTION III - RETURN ON TRAINING INVESTMENT

1. How would you describe the trade-off between the employee's time away from the job versus information technology / cyber security-related benefits from taking this course?

   Great benefits from training offset employee time away from the job
   Modest benefits from training offset employee time away from the job
   Benefits from training did not offset employee time away from the job
   Do not have enough information to respond
   Benefits from this course can not be measured in this manner

2. How would you respond if another employee from your area needed/wanted to take this course?

   Would definitely nominate others if I knew the course was applicable to their duties
   Would not nominate others because _____
   Would nominate others only if the following course changes were made:
   Do not have enough information to decide.

3. How knowledgeable were you about the course content before receiving this form?

   I had read the catalog description or brochure and knew the expected Learning Objectives.
   I had read the catalog description or brochure but did not know the expected Learning Objectives.
   I knew the overall purpose or goal of the course but did not read a detailed description of it and did not know the expected Learning Objectives.
   I only knew the course existed.
   I knew nothing about the course until I received this form.

4. As a supervisor, how satisfied are you with the training results from this course?

DRAFT

DRAFT

Appendix E: Glossary

- Awareness - the ability of the user to avoid behaviors that would compromise cyber security; practice good behaviors that will increase cyber security; and act wisely and cautiously, where judgment is needed, to increase cyber security.
- Awareness Training - managers must ensure that all users are provided awareness training, and that those identified as having significant responsibilities for information technology / cyber security are properly trained.
- Base knowledge - the familiarity, awareness, or understanding of security gained through experience or study.
- CIO – Chief Information Officer
- CISSO – Certified Information Systems Security Officer
- Competency - the quality of being adequately or well qualified physically and intellectually.
- Computer Literacy - an individual's familiarity with a basic set of knowledge with computers.
- Cyber security Learning Continuum - shows a progression of learning across the spectrum of roles within an organization.
- Definition - provides a definition of the function.
- Education - knowledge or skill obtained or developed by a learning process.
- FISMA – Federal Information Security Management Act
- FISSEA – Federal Information Systems Security Educators' Association
- IAM – Information Assurance Manager
- ISSO – Information Systems Security Officer
- IT – Information Technology
- ITL – the Information Technology Laboratory (ITL) at the National Institute of Learning Objectives(s): Identifies the outcomes the training module should strive to meet for each of the functions and their associated roles.

DRAFT

- Job Function - action for which a person or thing is particularly fitted or employed.
- Knowledge Unit – the combination of information needed to perform a function or activity effectively and efficiently.
- Literacy – an individual's familiarity with a basic set of knowledge.
- NIST – National Institute of Standards and Technology
- PM – Program Manager
- Proficiency - the state or quality of being competent
- Role - the responsibility and functions that a person is currently performing within their agency; are established by individual Federal Organization or Agency through position descriptions, hierarchy charts, responsibilities, etc.
- Role Areas - identifies various roles that are covered by the function. These roles are guidelines and may exist under different names within a particular Agency.
- SAISO – Senior Agency Information Security Officer
- Security Awareness - managers must ensure that all users are provided security awareness, and that those identified as having significant responsibilities for information technology / cyber security are properly trained.
- Security Literacy – an individual's familiarity with a basic set of knowledge with security principles and practices.
- Standards and Technology - develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology.
- Training - the action provided to a user in the acquisition of knowledge, skills, and competencies in the security arena.
- TWG – Technical Working Group

DRAFT

References

- FIPS 200 – entitled, "*Minimum Security Requirements for Federal Information and Information Systems,*" introduces awareness and training as one of the eighteen areas (called "families") of minimum security requirements identified to protect the confidentiality, integrity, and availability of Federal information systems and the information processed, stored, and transmitted by those systems.

- NIST SP 800-100 – entitled, "*Information Security Handbook: A Guide for Managers*" describes how to manage information security in your organization.

- NIST SP 800-16 – entitled, "*Information Technology Security Training Requirements: A Role- and Performance-Based Model*" was designed as a "living handbook" to provide information technology security training for Federal agencies.

- NIST SP 800-37 – entitled, "*Guide for Applying the Risk Management Framework to Federal Information Systems,"* addresses the risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, instructions, standards, Instructions, or regulations.

- NIST SP 800-50 – entitled, "*Building an Information Technology Security Awareness and Training Program,"* describes the following key approaches of an information technology / cyber security awareness and training program that "Federal Organizations" (i.e., Federal agency / departments, Agencies or organizations) should follow.

- NIST SP 800-53, Revision 4 – entitled, *"Recommended Security Controls for Federal Information Systems,"* provides more detail to the awareness and training area identified in FIPS 200 and provides levels for each control, dependent upon the system categorization and corresponding baseline.

- NIST SP 800-53A – entitled, *"Guide for Assessing the Security Controls in Federal Information Systems,"* provides guidelines for the assessment of the effectiveness of implemented awareness and training controls within an organization.

DRAFT