# Preliminary Draft

## NIST Special Publication 800-16
## Revision 2

# Cybersecurity Role Profiles for Training

**Warning Notice**

This document is a relatively cohesive document and is considered stable, although there are gaps in the content and the overall document is incomplete. Some changes are expected. Organizations may consider experimenting with guidelines, with the understanding that they will identify gaps and challenges. NIST welcomes early informal feedback and comments, which will be adjudicated after the specified public comment period; a full public draft is expected to follow.

**Original Release Date** June 27, 2019

INFORMATION SECURITY

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

# Preliminary Draft NIST Special Publication 800-16 Revision 2

# Cybersecurity Role Profiles for Training

William Newhouse
*Applied Cybersecurity Division*
*Information Technology Laboratory*

Kevin Sanchez-Cherry
*Office of the Chief Information Officer*
*Department of Transportation*

Clarence Williams
*Cyber Workforce Management*
*Department of Veterans Affairs*

Leo Van Duyn
*JP Morgan Chase & Co.*
*Columbus, OH*

June 2019

U.S. Department of Commerce
*Wilbur L. Ross, Jr., Secretary*

National Institute of Standards and Technology
*Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology*

## Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information 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.

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, Revision 2
Natl. Inst. Stand. Technol. Spec. Publ. 800-16, Revision 2, 45 pages (June 2019)
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. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

**Public comment period: June 27, 2019 through August 27, 2019**

National Institute of Standards and Technology
Attn: National Initiative for Cybersecurity Education
Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2002) Gaithersburg, MD 20899-2002
Email: niceframework@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

## 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

Today's cybersecurity workforce performs tasks in at least one of the work roles identified in the NICE Framework and is focused on reducing cybersecurity risk to an organization's operational technology (OT) such as industrial control systems (ICS), cyber-physical systems (CPS), Supervisory Control and Data Acquisition (SCADA) systems, and/or information technology (IT) systems.

This publication describes how to develop cybersecurity Role Profiles that can subsequently be used to identify existing training or develop new training.

This publication should be read, reviewed, or understood at a fairly high level by several audiences including the Organizational Heads through the leadership chain to the individual for whom the role profile applies.

## Keywords

cybersecurity; competency; learning continuum; proficiency, role profile; training.

## Supplemental Content

Please visit the NICE Framework website [1] to examine the NICE Framework and its supporting materials and tools such as the Reference Spreadsheet for the NICE Framework [2] and the NICE Framework Pivot Tool [3].

## Acknowledgments

NIST wishes to thank all individuals who have provided input to this version of the publication.

## Audience

Target Audience for this publication are:

- Management: All levels of management who are responsible for their staff training needs; prioritization of the use of training resources, identifying training gaps and understanding the value of the training in support of the mission of the organization.;
- Subject Matter Experts: Those with experience in performing cybersecurity work within one or more of the categories of the NICE Framework who can assist in developing cybersecurity role profiles and in identifying training to meet the requirements of the role profiles; identify training gaps and needs within the organization's Cybersecurity program; contributes to determining any customization that is needed and developing a compliance baseline, if necessary, for the organization; and
- Training Professionals: This group includes human resource planners, training coordinators/curriculum developers, course developers, and, of course the trainers responsible for developing, presenting and evaluating the training. This publication will show how to develop cybersecurity role profiles to be used by training professionals also known as those in the learning department to create and deliver the role-based training needed by an organization.

## Note to Reviewers

This publication introduces a spreadsheet tool known as the NICE Framework Pivot Tool. As the name implies, the ability to use pivot tables is necessary to examine the components in the NICE Framework that allow for the creation of cybersecurity role profiles. This publication also introduces cybersecurity competencies as a new component of the NICE Framework. Previously, the components of the NICE Framework included Categories, Specialty Areas, and Work Roles. The Work Roles include Knowledge, Skill, and Ability statements as well as tasks.

## Trademark Information

All trademarks or registered trademarks belong to their respective organizations.

## Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: niceframework@nist.gov

## Table of Contents

## List of Appendices

## List of Figures

## List of Tables

## Executive Summary

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce, is a partnership between government, academia, and the private sector working to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our nation secure.

NICE is committed to cultivating an integrated cybersecurity workforce that is globally competitive from hire to retire and prepared to protect our nation from existing and emerging cybersecurity challenges. NICE promotes nationwide initiatives that increase the number of people with the knowledge, skills, and abilities to perform the tasks required for cybersecurity work.

As threats that exploit vulnerabilities in our cyberinfrastructure grow and evolve, a cybersecurity workforce must be capable of designing, developing, implementing, and maintaining defensive and offensive cyber strategies. A workforce includes technical and nontechnical roles that are staffed with knowledgeable and experienced people. A cybersecurity workforce can address the cybersecurity challenges inherent to preparing their organizations to successfully implement aspects of their missions and business processes connected to cyberspace.

Role-based training can be leveraged as part of a learning continuum that prepares personnel to perform the cybersecurity work needed by an organization. A vital step for role-based training is to develop a role profile to inform identification or creation of role-based training.

This publication provides a process for developing cybersecurity role profiles using competencies, a new component added to the NICE Framework [1]. A user of the NICE Framework via the processes described in this publication now can document cybersecurity role profiles for role-based training purposes. This affirms the NICE Framework's function as reference resource to use as the starting point for workforce management guidance and guidelines aimed at strengthening an organization's ability to communicate consistently and clearly about cybersecurity work and its cybersecurity workforce.

Today's cybersecurity workforce includes those whose principal work involves performing tasks in at least one of the 52 work roles identified in the NICE Framework.  Such a workforce is focused on reducing cybersecurity risk to an organization's operational technology (OT) such as industrial control systems (ICS), cyber-physical systems (CPS), Supervisory Control and Data Acquisition (SCADA) systems, and/or information technology (IT) systems.

# 1 Introduction

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, is a partnership between government, academia, and the private sector that seeks to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our nation secure and economically competitive.

NICE is committed to cultivating an integrated cybersecurity workforce that is globally competitive from hire to retire, prepared to protect our nation from existing and emerging cybersecurity challenges.

Throughout this publication, the combined terms “cybersecurity workforce” is shorthand for a workforce with work roles that have an impact on an organization’s ability to reduce risk to its data, systems, and operations.

A cybersecurity workforce includes not only technically focused staff, but also those who apply knowledge of cybersecurity when preparing their organization to successfully implement its mission. This means that a cybersecurity worker may not work for the Chief Information Officer or Chief Information Security Officer in an organization. A cybersecurity worker could be in contracting or in the office of general counsel. A knowledgeable and skilled cybersecurity workforce is needed to address cybersecurity risks within an organization’s overall risk management process.

Individuals in the cybersecurity workforce will need training to develop skills that allow them to demonstrate cybersecurity competencies needed by their organization.

## 1.1 Purpose

This publication serves as a guide to the development of cybersecurity role profiles for training.

## 1.2 Scope

This publication describes the development of cybersecurity role profiles to inform the identification or creation of the role-based training. The publication a new component to the NICE Framework [1], a fundamental resource to improve the communication needed to identify, recruit, and develop cybersecurity talent. This publication is focused on developing role-based profiles used for role-based training which is one means to develop cybersecurity talent.

## 1.3 Audience

Developing cybersecurity role profiles that can be used in the planning for the development, implementation and evaluation of role-based training within an organization is an essential function of management. All levels of management should understand the necessity of role-based training and how role profiles for cybersecurity responsibilities are identified or described within their organization. This publication should be read, reviewed, understood, and supported by several key audiences to include CIO, CISO, IT senior managers/leadership, and other individuals who understand the cybersecurity work performed to reduce cybersecurity risk. Target audience includes:

- Cybersecurity workers who have responsibility for reducing cybersecurity risk. Some cybersecurity workers will bring their subject matter expertise to the development process, others are simply those who seek the training they need to perform their cybersecurity work;
- Cybersecurity training personnel tasked with designing role-based training courses or modules for personnel who have been identified as having significant cybersecurity responsibilities; and
- Training developers tasked with developing role-based training material, courses, or modules.

## 1.4 Assumptions

Personnel identified as having significant responsibility for Cybersecurity should receive role-based training to help their organizations address cybersecurity responsibilities.

## 1.5 Key Terms

It is important to define key terms that will be used and discussed throughout this publication. These definitions are for use in this publication and have been developed to provide clarity to the reader.

*Ability* - competence to perform an observable behavior or a behavior that results in an observable product

*Competency* - the capability of applying or using knowledge, skills, abilities, behaviors, and personal characteristics to successfully perform critical work tasks, specific functions, or operate in a given cybersecurity role or position

*Competency Group* - a grouping of like *Competencies; the four groups are Technical, Organization, Leadership, and Professional.*

*Cybersecurity Essentials* - the transitional stage between “Basic Awareness” and “Role-based Training.” It provides the foundation for subsequent specialized or role-based training by providing a baseline of key security terms and concepts

*Education* - knowledge or skill obtained or developed by a learning process as part of a planned, prepared, and coordinated program

*Knowledge* - a body of information applied directly to the performance of a function

*Proficiency* - the state or quality of being competent

*Proficiency Expectations* – the target proficiency for a competency or KSA in a role profile

*Role* - the responsibilities that a person has and the functions that a person is currently performing within their organization

*Role-profile* – a description of the competency, and KSA proficiencies expectations to be used by training course or module designers

*Role-profile Owner* - the person or persons responsible for creating and maintaining the *role profile*. They are most often subject matter experts for the cybersecurity work being performed in a *Role*.

*Skills* - the ability to do something

*Tasks* - specific defined piece of work that, combined with other identified Tasks, composes the work performed in a specific specialty area or work role in the NICE Framework.

*Training* - involves teaching, or developing in oneself or others, any skills and knowledge that relate to specific, useful cybersecurity competencies

*Work Role* - (from the NICE Framework) the most detailed groupings of cybersecurity work which include a list of attributes required to perform that role in the form of knowledge, skills, and abilities (KSAs) and tasks performed in that role.

### 1.6 Organization of this Special Publication

The remainder of this special publication is organized as follows:

- Section 2 provides the context for role profiles and the utilization of role-based training in a cybersecurity learning continuum.

- Section 3 is focused on role-prole creation showing how to engage the NICE Framework [1] as a reference resource via the NICE Framework Pivot Tool [3] to develop role profiles. The role profiles inform the design or selection of role-based training. Significantly, Section 3 introduces cybersecurity competencies as a new component of the NICE Framework.

- Section 4 offers roles and responsibilities for those who are in a position to leverage role-based training to prepare individuals to perform cybersecurity work.

- Appendix A list the top competencies for each NICE Framework Category

- Appendix B lists all the competencies which comprise a new component of the NICE Framework

- Appendix C provides references including the link to the NICE Framework Pivot Tool.

# 2 Cybersecurity Learning Continuum

The context where cybersecurity role profiles are being used for role-based can be expressed via a cybersecurity learning continuum. This publication is focused on enabling the use of one type of training, role-based training, to prepare an individual to perform cybersecurity tasks needed by an organization.

Figure 1, below, offers a visualization of that learning continuum and includes two workforces. “All Users” includes everyone who interacts with computing devices that are networked. Moving right, “All Cyber Roles” and “Work Roles” are people in your cybersecurity workforce performing tasks that have an impact on an organization’s ability to reduce the risk to its data, systems, and operations. This includes data and operations supported by the organization’s reliance on operational technology (OT) industrial control systems (ICS), cyber-physical systems (CPS), Supervisory Control and Data Acquisition (SCADA) systems, and/or information technology (IT) systems to performs its mission.

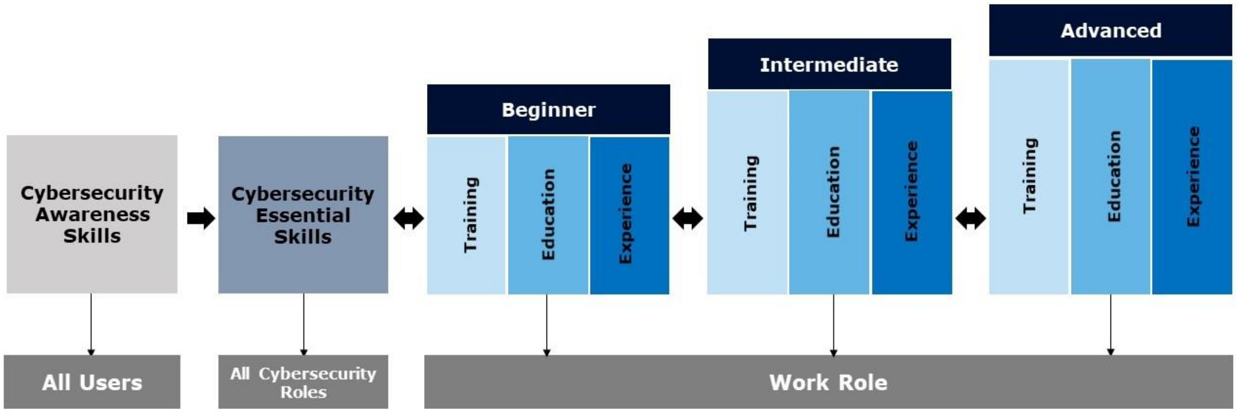


**Figure 1 Cybersecurity Learning Continuum**

## 2.1 Cybersecurity Awareness Training

The purpose of Cybersecurity Awareness Training is to focus attention on and establish recognition of the importance of cybersecurity, best practices, and individual responsibilities related to an individual’s interactions with computing devices that are networked or providing vital data used by an organization. Cybersecurity Awareness Training is intended to inform ALL USERS on how to recognize cybersecurity concerns and respond accordingly. In this publication, we are intentionally using the terms “Cybersecurity Awareness Training” instead of “Security Awareness Training” to be more specific to the cybersecurity domain and to avoid conflating the training with security awareness training for other domains.

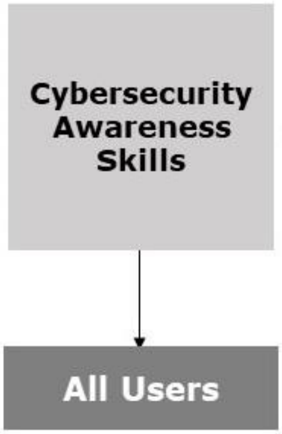


**Figure 2 Cybersecurity Awareness**

Cybersecurity awareness training seeks to focus an individual's attention on one issue or a set of issues and are_informed of the threats and vulnerabilities that impact their organization and personal work environments by explaining the "what" and "why" of cybersecurity. Communication of applicable cybersecurity policies, procedures and rules of behavior for use of an organization's systems establish a level of expectation on acceptable use and any sanctions and disciplinary actions imposed for noncompliance.

The fundamental value of cybersecurity awareness training is they help bring about a cultural change in attitudes that cybersecurity is everyone's responsibility. Pushing for the entire organization, all users, to realize that cybersecurity is critical and that cybersecurity failures have adverse consequences for everyone.

Detailed guidance on cybersecurity awareness is outside the scope of this draft revision of NIST SP 800-16, "*Cybersecurity Role Profiles for Training.*" It has previously been covered in more depth in NIST SP 800-50 "*Building an Information Technology Security Awareness and Training Program*".

Cybersecurity awareness training has been the focus of the annual conference of the Federal Information Systems Security Educators Association (FISSEA) which for 32 years has brought together visionaries, experts, and beginners from industry, academia, and government to discuss and share leading practices on improving cybersecurity awareness skills for everyone in an organization. Many private sector industries, organizations, and academia offer some form of cybersecurity awareness training to their employees, customers, and students.

## 2.2 Cybersecurity Essentials

Cybersecurity Essentials is the foundation that precedes the training, education, and experience necessary to prepare an individual for a specific work role within cybersecurity. This foundation is required before the individual can move forward in their learning.

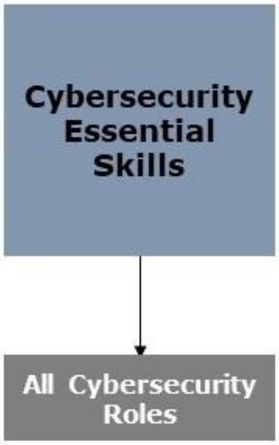


**Figure 3 Cybersecurity Essentials**

Cybersecurity Essentials, in addition to knowledge gathered via cybersecurity awareness training, provides a general introduction to cybersecurity with core knowledge sets needed to perform cybersecurity work.

Cybersecurity Essentials is a pre-requisite for entrance into the cybersecurity workforce.

Cybersecurity Essentials include an understanding of those key terms, essential concepts and principles relevant to all cybersecurity work role(s). These can be knowledge statements as described in the NICE Framework and can be determined by an organization's prioritization of relevant cybersecurity competencies in its cybersecurity workforce.

### 2.2.1 Competencies and Knowledge Statements

Below are the most leveraged competencies based on mapping each of the KSAs from the NICE Framework [1] to a competency. These competencies could be explored using the NICE Framework Pivot Tool [3] as the foundation for identifying your organization's cybersecurity essentials.

- Vulnerabilities Assessment
- Infrastructure Design
- Information Systems/Network Security
- Risk Management
- Legal, Government, and Jurisprudence
- Information Management
- Computer Network Defense
- Information Technology Assessment
- Technology Awareness
- Threat Analysis
- System Administration
- Encryption

Refer to Appendix B for complete list of competencies. Section 3.2.4 offers an example use of the NICE Framework Pivot Tool [3].

Below are the most leveraged knowledge statements in the NICE Framework [1] that could be used as cybersecurity essentials:

- Knowledge of computer networking concepts and protocols, and network security methodologies.
- Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
- Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- Knowledge of cybersecurity and privacy principles.
- Knowledge of cyber threats and vulnerabilities.
- Knowledge of specific operational impacts of cybersecurity lapses.

## 2.3 Cybersecurity Work Roles

In the learning continuum, **Training, Education,** and **Experience** as shown below in Figure 4 are different ways individual can become proficient in the performance of cybersecurity work roles at beginner, intermediate, or advanced levels.

“Training” to perform cybersecurity work roles involves teaching, or developing in oneself or others, any skills and knowledge that relate to specific, useful cybersecurity competencies. The publication focuses on one step in developing role-based training and does not include other types of training.

This publication does not cover in any detail the ‘Education’ factor beyond a subsection that follows. Experience connects with this publication via the subject matter experts bringing their advanced proficiencies into the development process for the role profile as described in Section Three of this publication.

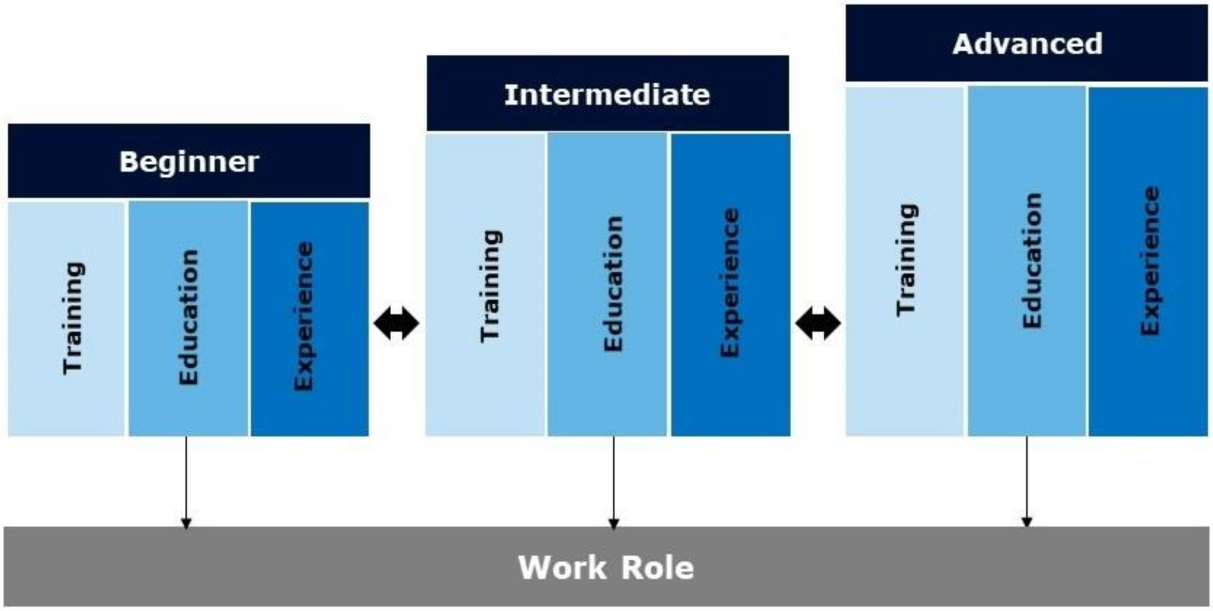


**Figure 4 Cybersecurity Work Role Proficiency Levels**

### 2.3.1 Role-Based Training

Role-based Training puts training in the context of a specific cybersecurity role profile. Role-based training allows one to deliver highly customized training content to one's cybersecurity workforce.

To leverage role-based training, a cybersecurity role profile needs to be developed.

A cybersecurity role profile can either be (1) an existing NICE Framework work role or (2) a custom crafted role profile that uses more components than those documented by a single work role in the NICE Framework. Picking which type of role profile to use is essentially asking if an existing NICE Framework work role describes the training needs of an individual with respect to an organization's needs. If not, a custom crafted role profile is needed.

In support of role-based training, this publication introduces competencies as a new component of the NICE Framework. Every KSA in the NICE Framework has been mapped to a single competency.

#### 2.3.1.1 Proficiency Levels

For purposes in this publication three proficiency levels are described.

- **Beginner** - Individual is developing an understanding of basic concepts in the field and acquiring formal or on-the-job training. No applied experience in this competency and requires close supervision to perform successfully.
- **Intermediate** - Individual is newly developing this competency and has completed formal training or on-the-job training. Demonstrates good theoretical knowledge of the

competency but has limited or no applied experience in this competency and requires a high level of guidance to perform successfully.
- **Advanced** - Individual has applied this competency independently in many situations. Capable of coaching others in the application of this competency.
- **None** - Individual does not demonstrate any proficiency in this competency.

### 2.3.2 Education and Experience

The Learning Continuum for cybersecurity includes **Education** and **Experience** along with **Training** to prepare an individual to perform cybersecurity roles.

**Education** can include industry-recognized IT security certification as well as the credentials like degrees and certificates offered by places of higher education.

**Experience** especially when it results in the ability to competently perform cybersecurity functions is highly valued. Students and workers can now leverage the preparation for and participation in cybersecurity competitions to gain experience that may not be part of their current cybersecurity roles.

Apprenticeships offer a system for preparing practitioners of cybersecurity with on-the-job training and often some accompanying study (classroom work and reading). Apprenticeships offer experience and is being used by more employers to fill cybersecurity positions.

The Learning continuum integrates training, education, and experience as means to prepare for cybersecurity roles.

# 3 Role Profile Creation

## 3.1 Using the NICE Framework to define Cybersecurity Roles

In this section, we introduce the steps used to identify/describe a role profile using the NICE Framework Pivot Tool that leverages the KSAs in the NICE Framework along with a mapping of those KSAs to competencies. The tool is a spreadsheet that requires the ability to use pivot table to identify the data used to describe a role profile.

A role profile can either be (1) an existing NICE Framework work role or (2) a custom crafted role profile to better match an individual or organizational need that uses more components of the NICE Framework than one of its work roles.

## 3.2 Creating a custom role profile – a worked example

Below we describe the steps to create a custom 'Cyber Defense Analyst' role profile.

The steps will likely be stewarded by the role profile owner(s), the learning department, and associated Subject Matter Experts (SMEs).

### 3.2.1 Defining the Role Profile

During a review of the organizational requirements for a role profile for a cyber defense analyst, SMEs determined that the role involved more than what is described by the NICE Framework work role titled "Cyber Defense Analyst". The SMEs believe that the role profile should also include competencies and associated KSAs in work roles found in three different Specialty Areas of the NICE Framework. In other words, the worked example's custom role profile includes competencies and KSAs not only aligned to the "Cyber Defense Analyst" NICE work role but also to the following specialty areas and their associated NICE work roles:

- **Cyber Operations (CO-OPS)** - Performs activities to gather evidence on criminal or foreign intelligence entities to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.
- **Cyber Defense Infrastructure Support (PR-INF)** - Tests, implements, deploys, maintains, reviews, 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.
- **Cyber Defense Analysis (PR-CDA)** - 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 to protect information, information systems, and networks from threats.

### 3.2.2 Determining Relevant Competencies for the Role Profile

By using the NICE Framework Pivot Tool [3], you can research which competencies are shared by the three NICE Framework Specialty Areas (CO-OPS, PR-INF, PR-CDA) identified above in section 3.2.1 and evaluate which ones are most relevant for the role profile.

To fill our details for our role profile, we looked for competencies that shared the KSAs between our three identified Specialty Areas. An Analysis and review with our SMEs determined that our work role will be comprised of KSAs mapped to the following Competencies:

1. Vulnerabilities Assessment
2. Computer Network Defense
3. Infrastructure Design
4. Information Systems/Network Security
5. System Administration
6. Network Management
7. Encryption
8. Threat Analysis
9. Information Assurance
10. Operating Systems

#### 3.2.2.1 Competency Groups

An individual's need for role-based cybersecurity training will change as their responsibilities evolve. Over time, an individual's cybersecurity responsibilities may allow them to demonstrate competencies within technical, professional, organizational, and leadership competency groups.

Each competency added by this publication to the NICE Framework has been assigned to one of these four competency groups. The groups offer a simple means to document when a role profile is focused on one or more of the following competency groups:

- Technical
- Organizational
- Professional
- Leadership

In our worked example for a custom 'Cyber Defense Analyst' role profile, the ten competencies noted in section 3.2.2 are all **Technical** competencies.

The NICE Framework Competencies Tab in the NICE Framework Pivot Tool [3] shows all the KSA to competency mappings and indicates the competency group of each competency.

### 3.2.3 Applicable KSAs (Knowledge, Skills & Abilities) for the Role Profile

From the identified the competencies in Sec. 3.2.2, you can pick the KSAs that are applicable to your role profile.

Table 1 shows KSAs that are mapped against the first two competencies, 'Computer Network Defense' and 'Vulnerabilities Assessment', identified in Sec. 3.2.2. Table 1, shows a subset of all the KSA mapped to the two competencies. These are the ones that you and SMEs agree best describe your custom role profile.

**Table 1 Role Profile Competencies and KSAs**

| Competency | KSAs |
|---|---|
| Computer Network Defense | Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions. |
| Computer Network Defense | Knowledge of adversarial tactics, techniques, and procedures. |
| Computer Network Defense | Knowledge of the common attack vectors on the network layer. |
| Computer Network Defense | Knowledge of signature implementation impact for viruses, malware, and attacks. |
| Computer Network Defense | Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications. |
| Computer Network Defense | Skill in developing and deploying signatures. |
| Computer Network Defense | Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort). |
| Vulnerabilities Assessment | Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities. |
| Vulnerabilities Assessment | Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump). |
| Vulnerabilities Assessment | Knowledge of how to use network analysis tools to identify vulnerabilities. |
| Vulnerabilities Assessment | Knowledge of penetration testing principles, tools, and techniques. |
| Vulnerabilities Assessment | Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list) |
| Vulnerabilities Assessment | Skill in evaluating the adequacy of security designs. |
| Vulnerabilities Assessment | Skill in using protocol analyzers. |
| Vulnerabilities Assessment | Skill in recognizing and categorizing types of vulnerabilities and associated attacks. |
| Vulnerabilities Assessment | Skill in performing packet-level analysis. |

### 3.2.4 NICE Framework Pivot Tool

Figure 6, below, is a screenshot of the second tab of the NICE Framework Pivot Tool [3] with some areas highlighted to show the Competencies and KSAs associated with the custom ‘Cyber Defense Analyst’ role profile developed earlier in Sec. 3.2.

The PivotTable Fields (top right) can be ‘dragged’ into the areas below (FILTERS, ROWS COLUMNS, and VALUES).

The main spreadsheet pivot table output data (left side) shown in Figure 6 displays the data after the pivot table selections were executed in the following order:

1. Populate, the FILTERS area with ‘Category’ and ‘Specialty Area’ as shown in Figure 6
    a. Pull both ‘Category’ and ‘Specialty Area’ from the PivotTable Fields area into the FILTERS area.

2. Select Specialty Areas

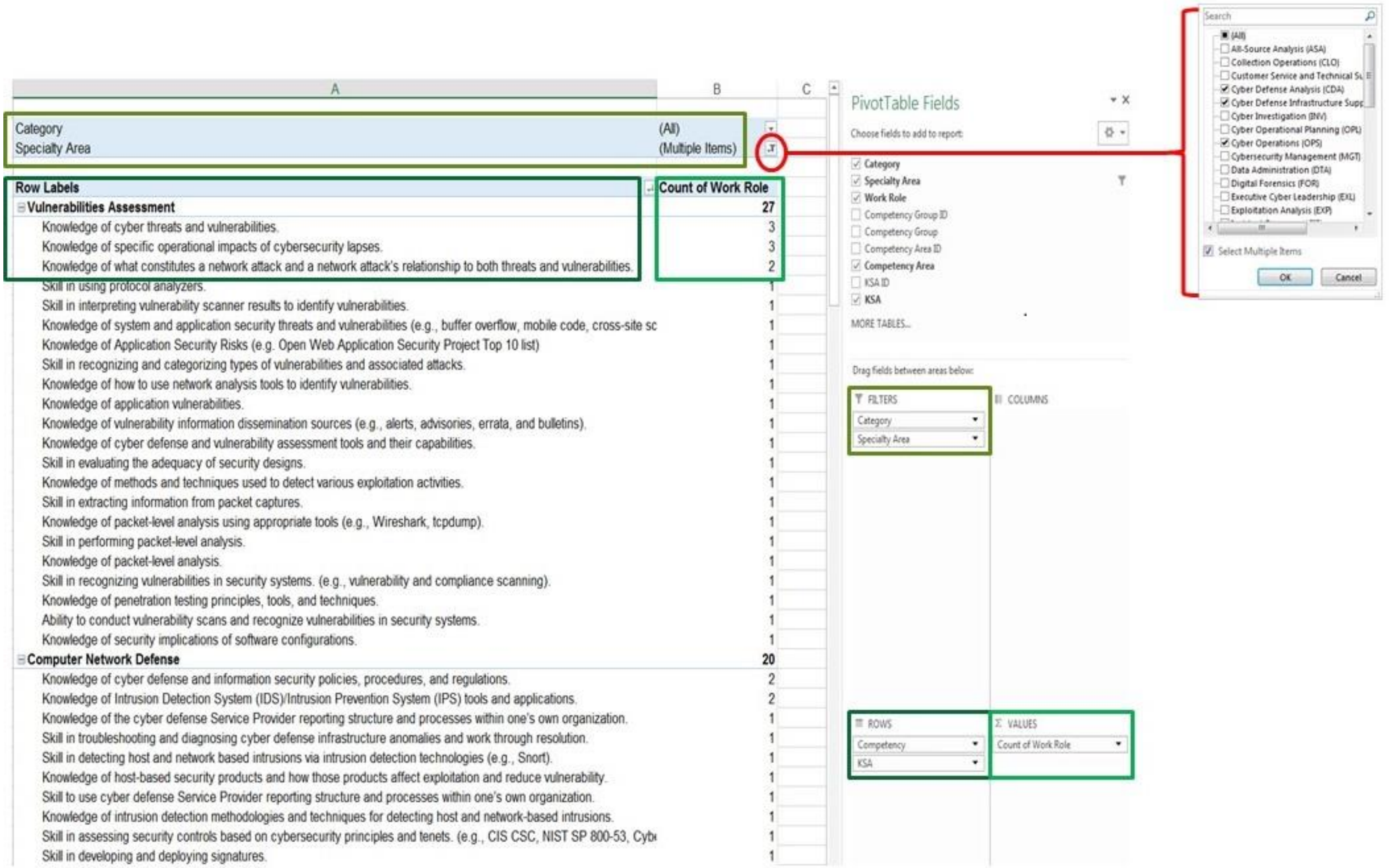
    a. Click the selection button in the very right of cell B3
    b. Click ‘All’ twice to deselect All
    c. Click to select the three Specialty Areas, (CO-OPS), Cyber Defense Infrastructure Support (PR-INF), and Cyber Defense Analysis (PR-CDA)

3. Sort by the most relevant competencies for the three Specialty Areas

    a. Pull only the “Competency” from the PivotTable Fields area into the ROWS area.
    b. Right click (default mouse or pointer settings) in cell B6, selecting ‘Sort’ and selecting Sort Largest to Smallest.

4. Add ‘KSA’ to the main spreadsheet pivot table output data
    a. Pull ‘KSA’ from the PivotTable Fields area to ROWS such that ‘KSA’ ends up below ‘Competency”

After completing these steps, FILTERS – Contain the fields of Category and Specialty Area; ROWS – Contain the fields of Competency and KSA; and VALUES – Shows the count of how many NICE Framework work roles include the KSA.



| | |
|---|---|
| Category | (All) |
| Specialty Area | (Multiple Items) |

| Row Labels | Count of Work Role |
|---|---|
| ⊟ **Vulnerabilities Assessment** | **27** |
| Knowledge of cyber threats and vulnerabilities. | 3 |
| Knowledge of specific operational impacts of cybersecurity lapses. | 3 |
| Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities. | 2 |
| Skill in using protocol analyzers. | 1 |
| Skill in interpreting vulnerability scanner results to identify vulnerabilities. | 1 |
| Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site sc | 1 |
| Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list) | 1 |
| Skill in recognizing and categorizing types of vulnerabilities and associated attacks. | 1 |
| Knowledge of how to use network analysis tools to identify vulnerabilities. | 1 |
| Knowledge of application vulnerabilities. | 1 |
| Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins). | 1 |
| Knowledge of cyber defense and vulnerability assessment tools and their capabilities. | 1 |
| Skill in evaluating the adequacy of security designs. | 1 |
| Knowledge of methods and techniques used to detect various exploitation activities. | 1 |
| Skill in extracting information from packet captures. | 1 |
| Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump). | 1 |
| Skill in performing packet-level analysis. | 1 |
| Knowledge of packet-level analysis. | 1 |
| Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning). | 1 |
| Knowledge of penetration testing principles, tools, and techniques. | 1 |
| Ability to conduct vulnerability scans and recognize vulnerabilities in security systems. | 1 |
| Knowledge of security implications of software configurations. | 1 |
| ⊟ **Computer Network Defense** | **20** |
| Knowledge of cyber defense and information security policies, procedures, and regulations. | 2 |
| Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications. | 2 |
| Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization. | 1 |
| Skill in troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution. | 1 |
| Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort). | 1 |
| Knowledge of host-based security products and how those products affect exploitation and reduce vulnerability. | 1 |
| Skill to use cyber defense Service Provider reporting structure and processes within one's own organization. | 1 |
| Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions. | 1 |
| Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cyb | 1 |
| Skill in developing and deploying signatures. | 1 |

PivotTable Fields

Choose fields to add to report:

☑ Category
☑ Specialty Area
☑ Work Role
☐ Competency Group ID
☐ Competency Group
☐ Competency Area ID
☑ Competency Area
☐ KSA ID
☑ KSA

MORE TABLES...

Drag fields between areas below:

FILTERS: Category, Specialty Area

COLUMNS

ROWS: Competency, KSA

Σ VALUES: Count of Work Role

Search

■ (All)
☐ All-Source Analysis (ASA)
☐ Collection Operations (CLO)
☐ Customer Service and Technical Su
☑ Cyber Defense Analysis (CDA)
☑ Cyber Defense Infrastructure Supp
☐ Cyber Investigation (INV)
☐ Cyber Operational Planning (OPL)
☑ Cyber Operations (OPS)
☐ Cybersecurity Management (MGT)
☐ Data Administration (DTA)
☐ Digital Forensics (FOR)
☐ Executive Cyber Leadership (EXL)
☐ Exploitation Analysis (EXP)

☑ Select Multiple Items

**Figure 5 NICE Framework Pivot Tool Example**

## 3.3 Proficiency Expectations

Proficiency level descriptions were given in Sec. 2.3.1.1 as beginner, intermediate, and advanced.

This publication does not offer guidance on how to determine proficiency expectations for a role profile as that is a qualitative assessment process performed locally by role profile owner(s), learning department, and associated SMEs.

The following variations of proficiency expectation are offered to note the flexibility one has in identifying proficiency expectations:

- One Proficiency - All Competencies and KSAs have the same proficiency expectation.
- Varied Competency Proficiencies - Each Competency identified in a role profile can have a different proficiency expectation.
- Varied KSA Proficiencies - Each KSA selected from a competency selected for a role profile can have a different proficiency expectation. For example, “knowledge” statements for a competency may be Intermediate while the “skill’ statements are Advanced.

### 3.3.1 Documenting Training Requirements based on your Role Profile

Training requirements will draw from the proficiency expectations for competencies and/or KSAs identified in your role profile.

Reviewing the role profile to select proficiency expectation is a collaborative effort between the role profile owner(s), learning department, and associated SMEs.

*Reminder: if a custom role profile is not needed, Appendix A, created using NICE Framework Pivot Tool, shows ten competencies for each NICE Framework.*

#### 3.3.1.1 Training Level Example

The role profile owner(s), the learning department, and associated SMEs have identified the following competencies as the focal points for the training program for our custom 'Cyber Defense Analyst' role profile development team:

1. Vulnerabilities Assessment
2. Computer Network Defense

Furthermore, the role profile owner(s), learning department, and associated SMEs have identified the KSAs for each competency that require development and selection of proficiency expectations. This is documented in Table 2.

Table 2 documents proficiency expectations for developing the training plan. The table can now be provided to your learning team to establish the training curriculum.

**Table 2 KSA Proficiency Expectations**

| Competency | KSAs | Proficiency Expectation | | |
|---|---|---|---|---|
| | | B | I | A |
| Computer Network Defense | Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions. | * | * | |
| Computer Network Defense | Knowledge of adversarial tactics, techniques, and procedures. | * | * | |
| Computer Network Defense | Knowledge of the common attack vectors on the network layer. | * | * | |
| Computer Network Defense | Knowledge of signature implementation impact for viruses, malware, and attacks. | * | * | |
| Computer Network Defense | Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications. | * | * | |
| Computer Network Defense | Skill in developing and deploying signatures. | * | * | * |

| Competency | KSAs | Proficiency Expectation | | |
|---|---|---|---|---|
| | | B | I | A |
| Computer Network Defense | Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort). | * | * | * |
| Vulnerabilities Assessment | Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities. | * | | |
| Vulnerabilities Assessment | Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump). | * | * | |
| Vulnerabilities Assessment | Knowledge of how to use network analysis tools to identify vulnerabilities. | * | * | |
| Vulnerabilities Assessment | Knowledge of penetration testing principles, tools, and techniques. | * | * | |
| Vulnerabilities Assessment | Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list) | * | | |
| Vulnerabilities Assessment | Skill in evaluating the adequacy of security designs. | | * | |
| Vulnerabilities Assessment | Skill in using protocol analyzers. | | * | |
| Vulnerabilities Assessment | Skill in recognizing and categorizing types of vulnerabilities and associated attacks. | | * | |
| Vulnerabilities Assessment | Skill in performing packet-level analysis. | | * | |

KEY: B - Beginner, I - Intermediate, A - Advanced, E - Expert

# 4 Responsibilities

The following positions if applicable to your organization, should be included in the development of cybersecurity role profiles for training. For each title, there are a list of "should's".

## 4.1 Organization Head

Heads of organizations must ensure that high priority is given to effective role-based training for their workforce. With regards to cybersecurity training, an organization head such as Chief Executive Officer (CEO) or President should:

- Ensure resources and budgets are available to support the cybersecurity training;
- Measure the effectiveness of the cybersecurity program; and
- Ensure that the agency has sufficiently trained personnel prepared to address cybersecurity risk.

## 4.2 Chief Information Officer (CIO)

Federal CIOs are tasked under FISMA to administer training and oversee personnel with significant cybersecurity responsibilities. Private sector CIOs likely have a similar responsibility within an organization. With regards to cybersecurity training, a CIO should help:

- Develop strategic plans that include a cybersecurity training;
- Communicate the importance of cybersecurity throughout all levels of the organization;
- Acquire and manage resources that support an effective cybersecurity training;
- Ensure that personnel throughout the organization are provided sufficient cybersecurity training to comply with applicable policies, procedures, standards, and guidelines; and
- Monitor and evaluate the effectiveness of the cybersecurity training.

## 4.3 Chief Information Security Officer (CISO)

CISO's have the responsibility of helping establish and maintain effective security within an organization and is compliant with policies and regulations. With regards to cybersecurity training, CISOs should help:

- Develop and maintain cybersecurity training;
- Advise senior management (e.g. CIO) on necessary training resources to support cybersecurity goals and objectives;
- Identify and fill of skills gaps via training;
- Provide direction to training objectives aimed at raising employee performance; and
- Develop a formal metrics process that measure the effectiveness of the cybersecurity training.

### 4.4 Cybersecurity Workforce Developer and Manager

Cybersecurity Workforce Developer and Managers have the responsibility of developing training and education requirements to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements. With regards to cybersecurity training, a Cybersecurity Workforce Developer and Manager should help:

- Advocate for adequate funding for cybersecurity training resources, to include both internal and industry-provided courses, instructors, and related materials;
- Support the CIO in meeting organizational cybersecurity training goals and objectives.
- Advise executive leadership on developmental training needs;
- Conduct learning needs assessments and identify requirements to support effective cybersecurity training;
- Develop or assist in the development of training policies and protocols for cybersecurity training;
- Establish and collect metrics to monitor and validate cybersecurity workforce readiness including analysis of cybersecurity workforce data to assess the status of positions identified, filled, and filled with qualified personnel, and
- Review/Assess cybersecurity workforce effectiveness to adjust skill and/or qualification standards.

### 4.5 Cyber Instructor

Cyber Instructors have the responsibility of developing and conducting training of personnel within cyber domain. With regards to cybersecurity training, a Cyber Instructure should help:

- Assist in the development of cybersecurity program learning objectives and goals;
- Ensure that training meets the goals and objectives for cybersecurity training;
- Prepare and deliver briefings to ensure that systems, network, and data users are aware of and adhere to systems security policies and procedures;
- Conduct interactive training exercises to create an effective learning environment;
- Develop new or identifying training materials that are appropriate for intended audiences;
- Help to evaluate the effectiveness and comprehensiveness of existing training programs;
- Design training curriculum and course content based on requirements; and
- Develop or assist in the development of written tests for measuring and assessing learner proficiency.

### 4.6 Cyber Instructional Curriculum Developer

Cyber Instructional Curriculum Developer develop, plan, coordinate, and evaluate cybersecurity training courses, methods, and techniques based on instructional needs. With regards to cybersecurity training, a Cyber Instructional Curriculum Developer should help:

- Create interactive learning exercises to create an effective learning environment;
- Develop or assist in the development of cybersecurity training policies and protocols;

- Develop the goals and objectives for cybersecurity training courses;
- Plan instructional strategies such as lectures, demonstrations, interactive exercises, multimedia presentations, video courses, web-based courses for most effective learning environment in conjunction with trainers;
- Connect training to business or mission requirements;
- Create training courses tailored to the audience and physical environment; and
- Conduct periodic reviews/revisions of course content for accuracy, completeness alignment, and currency (e.g., course content documents, lesson plans, student texts, examinations, schedules of instruction, and course descriptions).

## 4.7 Information Systems Security Manager (ISSM)

ISSMs are responsible for the cybersecurity of a program, organization, system, or enclave. With regards to cybersecurity training, an Information Systems Security Manager should help:

- Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support cybersecurity goals and objectives and reduce overall organizational risk; and
- Provide leadership and direction to cybersecurity personnel by ensuring that cybersecurity training is provided to personnel commensurate with their responsibilities.

## 4.8 Privacy Compliance Manager

Privacy Compliance Managers develop and oversee privacy compliance program and privacy program staff supporting the privacy compliance, governance/policy, and incident response needs of executives. With regards to cybersecurity training, a Privacy Compliance Manager should help:

- Include policy, plans, and strategy in compliance with laws, regulations, policies, and standards into organizational cybersecurity training activities;
- Coordinate with the Chief Information Security Officer to ensure alignment between security and privacy practices in training offerings;
- Conduct on-going privacy training activities;
- Include awareness of sanctions that can be applied for failure to comply with the corporate privacy policies and procedures in training offerings; and
- Include procedures for documenting and reporting self-disclosures of any evidence of privacy violation in training offerings.

## 4.9 Cybersecurity Personnel

Cybersecurity personnel include anyone whose work primarily involves performing the tasks described in the NICE Framework who their organization’s ability to reduce risk to its data, systems, and operations. With regards to cybersecurity training, an individual performing cybersecurity work should:

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

- Advise their management of additional training that can help them reduce cybersecurity risk faced by their organization; and
- Apply what is learned during role-based training; and document and record all training received.

Section Three of this document noted that a role profile owner(s), the learning department, and associated SMEs would work together to develop role profiles.  People in positions noted above may be included as SMEs in section Three.

## Appendix A—Competencies for each NICE Framework Category

The following data is based on analysis of data found in the NICE Framework using the NICE Framework Pivot Tool. It can be tailored for custom role profiles to meet the needs of an organization by the process described in Section Three of this publication.

The format for data in this Appendix is as follows:

- **Category:** A high-level grouping of common cybersecurity functions
- **Definition:** Provides a definition of the Category
- **Specialty Areas:** Distinct areas of cybersecurity work commonly found in the Category.
- **Work Role:** These are common functions found under the Specialty Area; these may exist under different names within a particular agency.
- **Primary Competencies**: Provides a list of the top leveraged KSA (Knowledge, Skill, Ability) areas for the work roles found in the category. The list came from use if the NICE Framework Pivot Tool.

**Category**: Analyze (AN)

**Definition -** Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

**Specialty Areas**:

- Threat Analysis (AN-TWA)
- Exploitation Analysis (AN-EXP)
- All-Source Analysis (AN-ASA)
- Targets (TGT)
- Language Analysis (LNG)

**Work Roles:**

- Threat/Warning Analyst (AN-TWA-001)
- Exploitation Analyst (AN-EXP-001)
- All-Source Analyst (AN-ASA-001)
- Mission Assessment Specialist (AN-ASA-002)
- Target Developer (AN-TGT-001)
- Target Network Analyst (AN-TGT-002)
- Multi-Disciplined Language Analyst (AN-LNG-001)

**Primary Competencies (Refer to Appx B for Competency Descriptions)**

1. Target Development
2. Intelligence Analysis
3. Threat Analysis
4. Data Analysis
5. Infrastructure Design
6. Telecommunications

7. Operations Support
8. Data Management
9. Vulnerabilities Assessment
10. Critical Thinking

**Category**: Collect and Operate (CO)
**Definition** - Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
**Specialty Areas**:

- Collection Operations (CO-CLO)
- Cyber Operational Planning (CO-OPL)
- Cyber Operations (CO-OPS)

**Work Roles**:

- All Source-Collection Manager (CO-CLO-001)
- All Source-Collection Requirements Manager (CO-CLO-002)
- Cyber Intel Planner (CO-OPL-001)
- Cyber Ops Planner (CO-OPL-002)
- Partner Integration Planner (CO-OPL-003)
- Cyber Operator (CO-OPS-001)

**Primary Competencies (Refer to Appx B for Competency Descriptions)**

1. Operations Support
2. Organizational Awareness
3. Data Management
4. Infrastructure Design
5. Threat Analysis
6. Telecommunications
7. Vulnerabilities Assessment
8. Interpersonal Skills
9. Information Management
10. Computer Network Defense

**Category**: Investigate (IN)
**Definition** - Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.
**Specialty Areas**:

- Cyber Investigation (IN-INV)
- Digital Forensics (IN-FOR)

**Work Roles**:

- Cyber Crime Investigator (IN-INV-001)
- Forensics Analyst (IN-FOR-001)
- Cyber Defense Forensics Analyst (IN-FOR-002)

**Primary Competencies (Refer to Appx B for Competency Descriptions)**

1. Computer Forensics
2. Legal, Government, and Jurisprudence
3. Vulnerabilities Assessment
4. Threat Analysis
5. System Administration
6. Operating Systems
7. Information Systems/Network Security
8. Computer Network Defense
9. Infrastructure Design
10. Computers and Electronics

**Category**: Operate and Maintain (OM)
**Definition** - Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
**Specialty Areas**:

- Data Administration (OM-DTA)
- Knowledge Management (OM-KMG)
- Customer Service and Technical Support (OM-STS)
- Network Services (OM-NET)
- Systems Administration (OM-ADM)
- Systems Analysis (OM-ANA)

**Work Roles**:

- Database Administrator (OM-DTA-001)
- Data Analyst (OM-DTA-002)
- Knowledge Manager (OM-KMG-001)
- Technical Support Specialist (OM-STS-001)
- Network Operations Specialist (OM-NET-001)
- System Administrator (OM-ADM-001)
- Systems Security Analyst (OM-ANA-001)

**Primary Competencies (Refer to Appx B for Competency Descriptions)**

1. Infrastructure Design
2. Vulnerabilities Assessment
3. Information Systems/Network Security
4. Data Privacy and Protection
5. System Administration
6. Encryption
7. Operating Systems
8. Risk Management
9. Enterprise Architecture
10. Information Management

**Category**: Oversee and Govern (OV)
**Definition** - Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
**Specialty Areas**:

- Legal Advice and Advocacy (OV-LGA)
- Training, Education, and Awareness (OV-TEA)
- Cybersecurity Management (OV-MGT)
- Strategic Planning and Policy (OV-SPP)
- Executive Cyber Leadership (OV-EXL)
- Project Management/Acquisition and Program (OV-PMA)

**Work Roles**:

- Cyber Legal Advisor (OV-LGA-001)
- Privacy Officer/Privacy Compliance Manager (OV-LGA-002)
- Cyber Instructional Curriculum Developer (OV-TEA-001)
- Cyber Instructor (OV-TEA-002)
- Information Systems Security Manager (OV-MGT-001)
- Communications Security (COMSEC) Manager (OV-MGT-002)
- Cyber Workforce Developer and Manager (OV-SPP-001)
- Cyber Policy and Strategy Planner (OV-SPP-002)
- Executive Cyber Leadership (OV-EXL-001)
- Program Manager (OV-PMA-001)
- Information Technology (IT) Project Manager (OV-PMA-002)
- Product Support Manager (OV-PMA-003)
- IT Investment/Portfolio Manager (OV-PMA-004)
- IT Program Auditor (OV-PMA-005)

**Primary Competencies (Refer to Appx B for Competency Descriptions)**

1. Vulnerabilities Assessment
2. Risk Management
3. Legal, Government, and Jurisprudence
4. Technology Awareness
5. Information Management
6. Information Systems/Network Security
7. Infrastructure Design
8. Information Technology Assessment
9. Organizational Awareness
10. Strategic Planning

**Category**: Protect and Defend (PR)
**Definition** - Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
**Specialty Areas:**

- Cyber Defense Analysis (PR-CDA)

- Cyber Defense Infrastructure Support (PR-INF)
- Incident Response (PR-CIR)
- Vulnerability Assessment and Management (PR-VAM)

**Work Roles:**

- Cyber Defense Analyst (PR-CDA-001)
- Cyber Defense Infrastructure Support Specialist (PR-INF-001)
- Cyber Defense Incident Responder (PR-CIR-001)
- Vulnerability Assessment Analyst (PR-VAM-001)

**Primary Competencies (Refer to Appx B for Competency Descriptions)**

1. Vulnerabilities Assessment
2. Computer Network Defense
3. Infrastructure Design
4. Information Systems/Network Security
5. Threat Analysis
6. Information Assurance
7. Incident Management
8. Network Management
9. Encryption
10. System Administration

**Category:** Securely Provision (SP)
**Definition** — Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
**Specialty Areas:**

- Risk Management (SP-RSK)
- Software Development (SP-DEV)
- Systems Architecture (SP-ARC)
- Systems Development (SP-SYS)
- Systems Requirements Planning (SP-SRP)
- Technology R&D (SP-TRD)
- Test and Evaluation (SP-TST)

**Work Roles:**

- Authorizing Official (SP-RSK-001)
- Security Control Assessor (SP-RSK-002)
- Software Developer (SP-DEV-001)
- Secure Software Assessor (SP-DEV-002)
- Enterprise Architect (SP-ARC-001)
- Security Architect (SP-ARC-002)
- Research and Development Specialist (SP-TRD-001)
- Systems Requirements Planner (SP-SRP-001)

- System Test & Evaluation Specialist (SP-TST-001)
- Information Systems Security Developer (SP-SYS-001)
- Systems Developer (SP-SYS-002)

**Primary Competencies (Refer to Appx B for Competency Descriptions)**

1. Information Assurance
2. Vulnerabilities Assessment
3. Infrastructure Design
4. Information Systems/Network Security
5. Systems Testing and Evaluation
6. Enterprise Architecture
7. Data Privacy and Protection
8. Risk Management
9. Systems Integration
10. Software Development

## Appendix B— NICE Framework Competencies

This appendix contains NICE Framework Competencies, Competency Groups, and their descriptions. All the KSAs in the NICE Framework have been mapped to one of these competencies.

**Table 3 NICE Framework Competencies**

| Competency | Competency Group | Description |
|---|---|---|
| Asset / Inventory Management | Technical | This area contains KSAs that relate to the process of developing, operating, maintaining, upgrading, and disposing of assets |
| Business Continuity | Operational | This area contains KSAs that relate to the planning and preparation of a company to make sure it overcomes serious incidents or disasters and resumes its normal operations within a reasonably short period |
| Client Relationship Management | Operational | This area contains KSAs that relate to the concepts, practices, and techniques used to identify, engage, influence, and monitor relationships with individuals and groups connected to a work effort—including those actively involved, those who exert influence over the process and its results, and those who have a vested interest in the outcome (positive or negative). |
| Collection Operations | Technical | This area contains KSAs that relate to executing collection using appropriate strategies and within the priorities established through the collection management process |
| Computer Forensics | Technical | This area contains KSAs that relate to the tools and techniques used in data recovery and preservation of electronic evidence. |
| Computer Languages | Technical | This area contains KSAs that relate to computer languages and their applications to enable a system to perform specific functions. |
| Computer Network Defense | Technical | This area contains KSAs that relate to the defensive measures to detect, respond, and protect information, information systems, and networks from threats. |
| Computers and Electronics | Technical | This area contains KSAs that relate to electronic data management or analysis devices, associated peripherals, accessories |
| Conflict Management | Professional | This area contains KSAs that relate to managing and resolving conflicts, grievances, confrontations, or disagreements in a constructive manner to minimize negative personal impact; collaborates with others to encourage cooperation and teaming. |
| Contracting/Procurement | Operational | This area contains KSAs that relate to the various types of contracts, techniques for contracting or procurement, and contract negotiation and administration. |
| Critical Thinking | Professional | This area contains KSAs that relate to the objective analysis of facts to form a judgment |

| Competency | Competency Group | Description |
|---|---|---|
| Data Analysis | Technical | This area contains KSAs that relate to collecting, synthesizing, and/or analyzing qualitative and quantitative data and information from a variety of sources to reach a decision, make a recommendation, and/or compile reports, briefings, executive summaries, and other correspondence. |
| Data Management | Technical | This area contains KSAs that relate to the development and execution of data management plans, programs, practices, processes, architectures, and tools that manage, control, protect, deliver, archive, dispose of, and enhance the value of data and information assets. |
| Data Privacy and Protection | Operational | This area contains KSAs that relate to the relationship between the collection and dissemination of data, technology, the public expectation of privacy, legal and political issues surrounding them |
| Database Administration | Technical | This area contains KSAs that relate to managing and maintaining database management systems (DBMS) software |
| Database Management Systems | Technical | This area contains KSAs that relate to the use of database management systems and software to control the organization, storage, retrieval, security, and integrity of data. |
| Encryption | Technical | This area contains KSAs that relate to the process of transforming information to make it unreadable for unauthorized users. |
| Enterprise Architecture | Technical | This area contains KSAs that relate to the principles, concepts, and methods of enterprise architecture to align information technology (IT) strategy, plans, and systems with the mission, goals, structure, and processes of the organization. |
| External Awareness | Operational | This area contains KSAs that relate to identifying and understanding how internal and external issues (e.g., economic, political, social trends) impact the work of the organization |
| Identity Management | Technical | This area contains KSAs that relate to the security and business discipline that "enables the right individuals to access the right resources at the right times and for the right reasons" |
| Incident Management | Technical | This area contains KSAs that relate to the tactics, technologies, principles, and processes to analyze, prioritize, and handle incidents. |
| Information Assurance | Technical | This area contains KSAs that relate to the methods and procedures that protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity. |
| Information Management | Technical | This area contains KSAs that relate to where or how to gather, organize, maintain, or modify information or information management systems to effectively process, store, and/or distribute information. |

| Competency | Competency Group | Description |
|---|---|---|
| Information Systems / Network Security | Technical | This area contains KSAs that relate to the methods, tools, and procedures, including development of information security plans to prevent information systems vulnerabilities and to provide or restore security of information systems and network services. |
| Information Technology Assessment | Technical | This area contains KSAs that relate to the principles, methods, and tools (for example, surveys, system performance measures) to assess the effectiveness and practicality of information technology systems. |
| Infrastructure Design | Technical | This area contains KSAs that relate to the architecture and typology of software, hardware, and networks, including LANS, WANS, and telecommunications systems, their components and associated protocols and standards, and how they operate and integrate with one another and with associated controlling software. |
| Intelligence Analysis | Technical | This area contains KSAs that relate to the process by which the information collected about an enemy is used to answer tactical questions about current operations or to predict future behavior. |
| Interpersonal Skills | Professional | This area contains KSAs that relate to developing and maintaining effective relationships with others; relating well to people from varied backgrounds and different situations. Considering and responding appropriately to the needs, feelings, and capabilities of subordinates, peers, and seniors. |
| Knowledge Management | Technical | This area contains KSAs that relate to the value of collected information and the methods of sharing that information throughout an organization. |
| Legal, Government, and Jurisprudence | Operational | This area contains KSAs that relate to laws, regulations, policies, and ethics that can impact organizational activities. |
| Mathematical Reasoning | Technical | This area contains KSAs that relate to devising strategies to solve a wide variety of math problems and determine if an assertion is correct. |
| Modeling and Simulation | Technical | This area contains KSAs that relate to mathematical modeling and simulation tools and techniques to plan and conduct test and evaluation programs, characterize systems support decisions involving requirements, evaluate design alternatives, or support operational preparation. |
| Network Management | Technical | This area contains KSAs that relate to the operation, management, and maintenance of network and telecommunication systems and linked systems and peripherals. |
| Operating Systems | Technical | This area contains KSAs that relate to computer network, desktop, and mainframe operating systems and their applications. |
| Operations Support | Technical | This area contains KSAs that relate to the policies and procedures to ensure production or delivery of products and services, including tools and mechanisms for distributing new or enhanced hardware and software. |

| Competency | Competency Group | Description |
|---|---|---|
| Oral Communication | Professional | This area contains KSAs that relate to the process of expressing information or ideas by word of mouth |
| Organizational Awareness | Operational | This area contains KSAs that relate to understanding an organization’s mission and functions, its social and political structure and how programs, policies, procedures, rules, and regulations drive and impact the work and objectives of the organization. |
| Policy Management | Operational | This area contains KSAs that relate to the process of creating, communicating, and maintaining policies and procedures within an organization |
| Presenting Effectively | Professional | This area contains KSAs that relate to the activity in which someone shows, describes, or explains something to an audience. |
| Problem Solving | Technical | This area contains KSAs that relate to determining the accuracy and relevance of information and using sound judgment to generate and evaluate alternatives; making well-informed, objective decisions that take into account facts, goals, constraints, and risks while perceiving the impact and implications of decisions. |
| Process Control | Operational | This area contains KSAs that relate to the active changing of the process based on the results of process monitoring. |
| Project Management | Leadership | This area contains KSAs that relate to the principles, methods, or tools for developing, scheduling, coordinating, and managing projects and resources, including monitoring and inspecting costs, work, and contractor performance. |
| Requirements Analysis | Technical | This area contains KSAs that relate to the principles and methods to identify, analyze, specify, design, and manage functional and infrastructure requirements—includes translating functional requirements into technical requirements used for logical design or presenting alternative technologies or approaches. |
| Risk Management | Operational | This area contains KSAs that relate to the methods and tools used for risk assessment and mitigation of risk. |
| Software Development | Technical | This area contains KSAs that relate to the collective processes involved in creating software programs, embodying all the stages throughout the systems development life cycle |
| Software Testing and Evaluation | Technical | This area contains KSAs that relate to the principles, methods, and tools for analyzing and administering software test and evaluation procedures, as well as technical characteristics of IT systems, including identifying critical operational issues. |
| Strategic Planning | Leadership | This area contains KSAs that relate to formulating effective strategies consistent with the objective, vision, and competitive strategy of the organization and/or business unit. |

| Competency | Competency Group | Description |
|---|---|---|
| System Administration | Technical | This area contains KSAs that relate to the upkeep, configuration, and reliable operation of computer systems. |
| Systems Integration | Technical | This area contains KSAs that relate to the principles, methods, and procedures for installing, integrating, and optimizing information systems components. |
| Systems Testing and Evaluation | Technical | This area contains KSAs that relate to the principles, methods, and tools for analyzing and administering systems test and evaluation procedures, as well as technical characteristics of IT systems, including identifying critical operational issues. |
| Target Development | Technical | This area contains KSAs that relate to the systematic examination of potential target systems, their components and the elements which make up each component in order to determine the importance, priority, weight of effort, and appropriate weapons selection for specific target systems. |
| Teaching Others | Leadership | This area contains KSAs that relate to imparting knowledge of or giving information about or instruction in (a subject or skill) |
| Technology Awareness | Technical | This area contains KSAs that relate to keeping up-to-date on technological developments and making effective use of technology to achieve results |
| Telecommunications | Technical | This area contains KSAs that relate to the transmissions, broadcasting, switching, control, and operation of telecommunications and/or telephony or conferencing systems and related network infrastructure. |
| Third Party Oversight / Acquisition Management | Operational | This area contains KSAs that relate to the process of analyzing and controlling risks presented to your company, data, operations and finances by parties other than your own company. |
| Threat Analysis | Technical | This area contains KSAs that relate to the process in which the knowledge of internal and external information vulnerabilities pertinent to a particular organization is matched against real-world cyber attacks. |
| Vulnerabilities Assessment | Technical | This area contains KSAs that relate to the principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures. |
| Web Technology | Technical | This area contains KSAs that relate to the principles and methods of web technologies, tools, and delivery systems, including web security, privacy policy practices, and user interface issues as they apply to development. |
| Workforce Management | Leadership | This area contains KSAs that relate to the activities needed to maintain a productive workforce |
| Written Communication | Professional | This area contains KSAs that relate to any type of message that makes use of the written word. |

# Appendix C—References

[1] NICE Framework, National Institute of Standards and Technology [Website], https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

[2] Reference Spreadsheet for the NICE Framework, NIST SP 800-181, [Excel File], https://www.nist.gov/document/supplementnicespecialtyareasandworkroleksasandtasksxlsx

[3] NICE Framework Pivot Took [Excel File], https://www.nist.gov/document/niceframeworkksatocompetencymappingxlsx