NIST Internal Report
NIST IR 8355

NICE Framework Competency Areas

Preparing a Job-Ready Cybersecurity Workforce

Karen A. Wetzel

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8355

.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Internal Report
NIST IR 8355

NICE Framework Competency Areas

Preparing a Job-Ready Cybersecurity Workforce

Karen A. Wetzel
NICE
Applied Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8355

June 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on 2023-06-01

How to Cite this NIST Technical Series Publication:
Wetzel KA (2023) NICE Framework Competency Areas: Preparing a Job-Ready Cybersecurity Workforce. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal or Interagency Report (IR) NIST IR 8355. https://doi.org/10.6028/NIST.IR.8355

Author ORCID iDs
Karen A. Wetzel: 0009-0004-0683-808X

Contact Information
niceframework@nist.gov

NICE
National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Abstract

This publication from NICE describes Competency Areas as included in the *Workforce Framework for Cybersecurity (NICE Framework)*, NIST Special Publication 800-181, Revision 1. The NICE Framework is a fundamental reference for describing and sharing information about cybersecurity work. At its core are Task, Knowledge, and Skill (TKS) statements that provide a foundation for learners, including students, job seekers, and employees. These statements are then used to define Competency Areas—clusters of related Knowledge and Skill statements that correlates with one's capability to perform Tasks in a particular domain—and Work Roles, which are composed of Task statements that constitute work for which someone is responsible or accountable. This document shares more detail about what NICE Framework Competency Areas are, including their evolution and development, clarifies the differences between Competency Areas and Work Roles, and provides example uses for Competency Areas from various stakeholder perspectives, and. Finally, the publication identifies where the NICE Framework list of Competency Areas is separately published and maintained distinct from this publication so it can be updated more frequently as a flexible and contemporary reference resource.

Keywords

competency; Competency Area; cyber; cybersecurity; cyberspace; education; knowledge; risk management; role; security; skill; task; team; training; workforce; work role.

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.

Audience

The NICE Framework serves as a bridge between employers and education, training, and certification providers as well as a tool to help learners determine needs and demonstrate capabilities. A standardized approach to Competency Areas provides accessible information about what individuals need to know and be able to do, enables the development of more effective learning, and establishes regular processes to consistently describe and validate a learner's capabilities. Therefore, the following are both stakeholders and the audience for this work: employers; workforce development and human resources professionals; education, training, and certification providers; and learners.

Document Conventions

The terms "shall" and "shall not" indicate requirements to be followed strictly in order to conform to the publication and from which no deviation is permitted. The terms "should" and "should not" indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms "may" and "need not" indicate a course of action permissible within the limits of the publication. The terms "can" and "cannot" indicate a possibility and capability, whether material, physical or causal.

Those seeking a career in cybersecurity or performing cybersecurity work—including students, job seekers, and employees—are referenced as Learners. This moniker highlights that each member of the workforce is also a lifelong learner.

Note to Readers

This publication assumes existing knowledge of the *Workforce Framework for Cybersecurity (NICE Framework)*, NIST Special Publication 800-181, Revision 1, and is expected to be read in that context. This document was released in draft form for comment twice prior to this publication. The first draft was released in March 2021, along with an initial list of proposed Competency Areas. A second draft was released in December 2021. Feedback received on those drafts, conversations with NICE community members, and insights from workshops that brought together subject matter experts on this topic have matured understanding of NICE Framework Competency Areas. The adjustments to this document are the result. Any subsequent draft(s) may be further adjusted, including the separately provided Competency Areas, their descriptions, and associated Task, Knowledge, and Skill (TKS) statements.

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Table of Contents

List of Tables

List of Figures

Acknowledgments

The National Institute of Standards and Technology (NIST) would like to particularly acknowledge the work of William Newhouse (NIST), Kevin Sanchez-Cherry (Department of Transportation), Leo Van Duyn (JPMorgan Chase & Co.), and Clarence Williams (Department of Veterans Affairs), whose work provided the basis from which this publication came. NIST also wishes to thank these team members from the NICE Framework Core Authoring Team that includes representatives from numerous departments and agencies in the United States Federal Government whose dedicated efforts contributed significantly to that publication:

Lisa Dorr, Department of Homeland Security
Ryan Farr, Department of Defense
Pam Frugoli, Department of Labor
Matt Isnor, Department of Defense
Patrick Johnson, Department of Defense
Rodney Petersen, National Institute of Standards and Technology
Danielle Santos, National Institute of Standards and Technology
Stephanie Shively, Department of Defense
Kenneth Vrooman, Cybersecurity and Infrastructure Security Agency

Finally, the team appreciates and acknowledges the contributions of those who established previous editions of cybersecurity workforce frameworks as described at the history page of the NICE Framework Resource Center.

1. Introduction

NICE released the *Workforce Framework for Cybersecurity (NICE Framework)*, NIST Special Publication 800-181, Revision 1, in November 2020 [1]. The revised NICE Framework established a set of building blocks—Task, Knowledge, and Skill statements—that describe cybersecurity work and what someone must know or be able to do to complete that work. It also identifies common ways these building blocks can be applied, most notably through Work Roles and, new in the NICE Framework revision 1, Competency Areas.[1]

NICE Framework Competency Areas group together related Task, Knowledge, and Skill (TKS) statements to form a higher-level description of capabilities typically needed in a particular cybersecurity domain. By clearly defining what a person needs to know and do to perform well in a defined area of cybersecurity work, Competency Areas provide a means to communicate the needs of employers, the capabilities of learners (which, for the purposes of the NICE Framework includes students, job seekers, and employees), and the value of education, training, and certifications.

> **Learners:** Individuals who perform cybersecurity work, including students, job seekers, and employees.

Competency Areas are defined via an employer-driven approach that enables education and training providers to be responsive to employer or sector needs by creating experiences that help learners develop and demonstrate relevant and needed capabilities. They correlate with performance on the job and can be improved through education, training (including on-the-job and apprenticeships), or other learning experiences.

1.1. Purpose

This publication provides readers background information on NICE Framework Competency Areas and why they were introduced in the revised NICE Framework, describes how the Competency Areas are defined and written, and shares with readers ways NICE Framework Competency Areas can be used.

1.2. Scope

The Competency Areas described in this publication are part of the *Workforce Framework for Cybersecurity (NICE Framework)*, which provides a lexicon for describing cybersecurity work and the individuals who do that work. The NICE Framework considers the "cybersecurity workforce" to include not only those whose primary focus is on cybersecurity but also those who need specific cybersecurity-related knowledge and skills to properly manage cybersecurity-related risks to the enterprise.

[1] The NICE Framework building block statements, Work Roles, and Competency Areas are made available online as part of the NICE Framework Resource Center in order to allow for regular review and updates [2].

2. Competency Areas and the NICE Framework

The introduction of Competency Areas into the NICE Framework is a response to a growing need to better identify and secure talent through skills- and competency-based hiring. Hiring based only on degrees increases the likelihood of excluding qualified candidates, particularly for jobs related to emerging technologies. A shift to competency-based hiring and promotion ensures that the individuals most capable of performing the roles and responsibilities required of a specific position are those selected for that position. With the inclusion of Competency Areas, the NICE Framework provides a means of helping the NICE Framework users shift to competency-based hiring practices.

Competency Areas use an employer-driven approach to group together related Knowledge and Skill statements that correlate with one's capability to perform Tasks in a particular domain. Over time, NICE may work with the cybersecurity community to introduce new Competency Areas or update or retire existing Competency Areas in response to evolving needs.

NICE Framework Competency Areas are complementary to Work Roles and provide a means to assess learner capabilities in the defined areas. (See *Section 2.3, Competency Areas and Work Roles*, for more information about how Competency Areas differ from and work in conjunction with Work Roles.)

2.1. Evolution of NICE Framework Competency Areas

NICE Framework Competency Areas were first introduced in the NIST Special Publication 800-181 in the 2020 revision, but they also derive from earlier work. The first version of the National Cybersecurity Workforce Framework 1.0 (April 2013), which preceded and formed the basis for NIST SP 800-181, included a mapping of Knowledge, Skill, and Ability (KSA) statements to "competencies."[2]

These competencies pulled from a 2011 U.S. Office of Personnel Management (OPM) memorandum that introduced a "Competency Model for Cybersecurity," which itself followed a coordinated effort with the Federal Chief Information Officers (CIO) Council and NICE in November 2009 [3].[3] The OPM model presented 117 competencies related to four occupation series and the pay grades of personnel in those occupations. A subject matter expert panel review of the OPM model conducted at that time identified 50 competencies to align with the NICE Framework KSAs found in five of the seven categories of work.[4]

Prior to publishing NIST SP 800-181in 2017, consideration was given as to whether competencies should be included, but it was decided not to maintain them as part of the NICE Framework at that time. Inclusion of competencies in the NICE Framework was revisited for the 2020 publication, when they were added to the publication as a means of applying TKS statements, along with Work Roles. In March 2021, a draft list of "competencies" was released for comment. Feedback received during that comment period, as well as stakeholder conversations held via a workshop and in other settings, informed the next stage of development, so that a clearer understanding of this new approach could be made. The result is a shift from

[2] Note that Ability statements were removed in the 2020 revision of the NICE Framework.
[3] Berry, J. (2011, February 16). U.S. Office of Personnel Management Memorandum. Competency model for cybersecurity. Retrieved February 11, 2021, from https://www.chcoc.gov/content/competency-model-cybersecurity [4]
[4] Two categories—"Collect and Operate" and "Analyze"—related to classified content and thus were not included in that alignment review.

"competencies" to the current "Competency Areas" described herein. Although the overall purpose of Competency Areas remains the same, this new phrasing better signals an approach that broadly defines the knowledge and skills one needs to be capable in a defined domain, distinct from one's proficiency in completing a single task. The list of Competency Areas themselves, though derived from and informed by earlier efforts, is an evolution of that work and will continue to be updated and adjusted in response to the shifting cybersecurity environment.[5]

2.2. Defining Competency Areas

Competency Areas offer a high-level perspective to defined areas of cybersecurity work and support an inclusive, assessment-based approach to determine capabilities. An assessment-based approach allows applicant pools to be broadened and to identify candidates more successfully, particularly in areas such as emerging and rapidly evolving technologies. They can also be used to identify career paths, to determine current and future workforce demands, and when developing education, training, or other learning experiences to meet defined needs.

> **Competency Area:** A cluster of related Knowledge and Skill statements that correlates with one's capability to perform Tasks in a particular domain. Competency Areas can help learners discover areas of interest, inform career planning and development, identify gaps for knowledge and skills development, and provide a means of assessing or demonstrating a learner's capabilities in the domain.
>
> Competency Areas consist of a name, description of the area, and group of associated TKS statements.

Accordingly, instead of specifying only the work to be done (Tasks) or what is needed to do the work (Knowledge and Skills), it's about determining a learner's overall capability for that area of cybersecurity work.[6] Competency Areas offer an opportunity to increase alignment and coordination between employers, learners, and education, training, and certification providers (see Fig. 1. NICE Framework Competency Area Stakeholders).

[5] The creation and maintenance of NICE Framework Competency Areas follows NIST practices of engaging with stakeholders in an open, transparent, and collaborative process that includes workshops and other opportunities to provide input. Information on how to engage with the NICE Framework, the revision process, and the current List of Competency Areas can be found in the NICE Framework Resource Center: https://www.nist.gov/nice/framework.

[6] See also the 2022 NICE Report to Congress, *Measuring Cybersecurity Workforce Capabilities: Defining a Proficiency Scale for the NICE Framework*. This report discusses proficiency levels broadly, points to existing models, summarizes findings regarding efforts to assess workforce proficiency, and provides recommendations for effective methods for measuring the cybersecurity proficiency of learners.

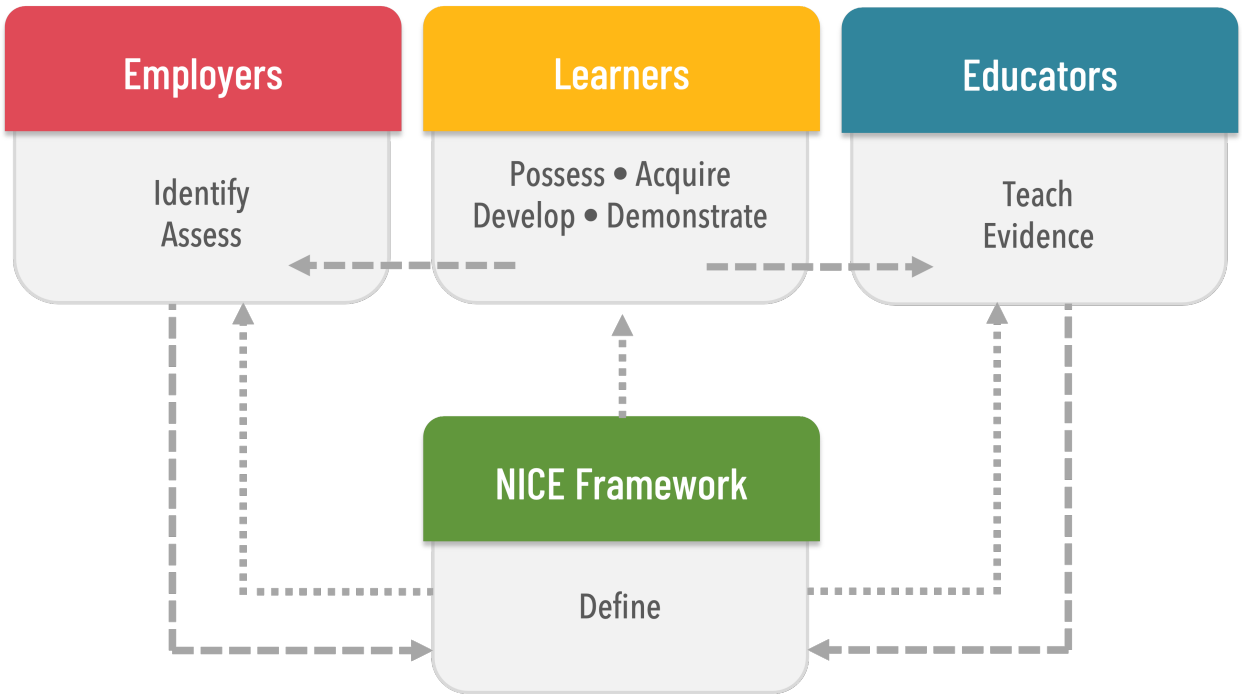


Fig. 1. NICE Framework Competency Area Stakeholders

2.3. Competency Areas and Work Roles

NICE Framework Competency Areas and Work Roles are complementary and may be used together or separately. However, there are differences. While Work Roles focus on the work to be done (Task statements), Competency Areas focus on what a learner must know or be able to do (Knowledge and Skill statements) to complete that work (see Fig. 2. TKS Statements, Competency Areas, and Work Roles).

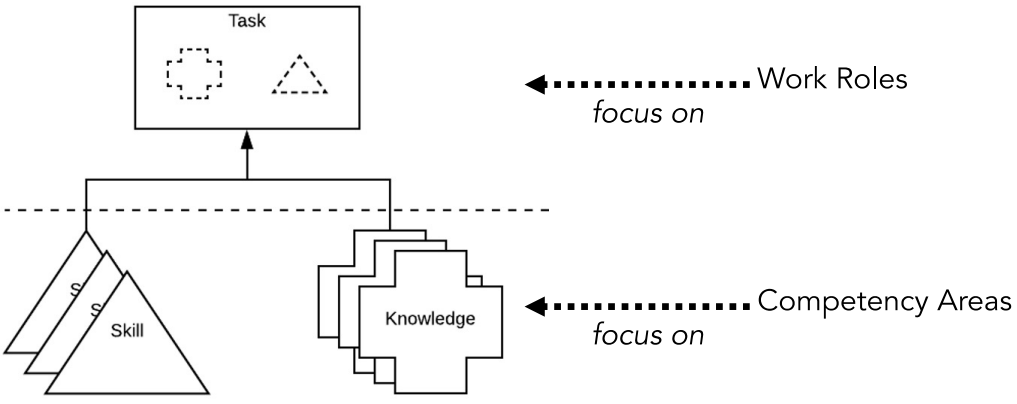


Fig. 2. TKS Statements, Competency Areas, and Work Roles

Competency Areas help address employers' capability needs more broadly, while Work Roles are used when defining specific positions and responsibilities. Finally, assessment is typically based on the Competency Area as a whole, whereas assessment for Work Roles typically occurs at the Task level.

Table 1. NICE Framework Competency Areas vs. Work Roles

Competency Areas	Work Roles
Learner focused	Work focused
Help address employer needs	Help define positions and responsibilities
Assessment is typically based on a Competency Area as a whole	Assessment typically occurs at the Task level

Work Roles represent a defined area of work that is commonly agreed upon in many different types of organizations and sectors. Competency Areas, however, may represent emerging areas that aren't yet broadly incorporated into defined Work Roles, capability that pulls from multiple Work Roles, and fundamental areas of expertise in cybersecurity.

3. Competency Area Development

The following guidelines are used for the development of individual Competency Areas as part of the NICE Framework. Competency Areas:

- May used **independently** of Work Roles
- May be **additive** to or overlaid onto one or more Work Roles
- May **span** multiple Work Roles (i.e., incorporate Knowledge and Skill statements from multiple Work Roles)
- May represent **emerging domains** that do not yet have established Work Roles

In addition, Competency Areas:

- **Do not duplicate** existing Work Roles

Competency Areas are made up of the following components:

1. **Competency Area Title:** The name of the Competency Area; the title clearly signals to all stakeholders the area that will be described.
2. **Competency Area Description:** The description should:
    a. **Begin with "This Competency Area describes a learner's capabilities related to…."** Using the same standard language to introduce each description serves as a signpost for readers that it is a Competency Area description while focusing the competency onto the learner at the onset.

b. **Define the Competency Area simply and clearly.** The Competency Areas should be defined using plain language. Anyone reading the description should be able to quickly and easily understand the scope and meaning of the Competency Area.

c. **Reflect content from TKS statements.** The description may echo language from Task, Skill, or Knowledge statements that are associated with the Competency Area, though it should not wholly duplicate that language.

d. **Balance specificity with broad application.** A goal of a NICE Framework Competency Area is to provide flexibility of application; the description should be detailed enough to clearly define its scope and meaning, but not so narrow as to restrict use by multiple stakeholders or time-date the competency (e.g., by referencing a particular computer program or coding language).

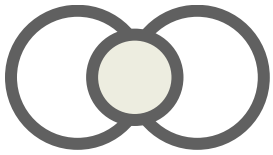
e. **Omit unnecessary qualifiers.** Qualifiers (e.g., "thorough knowledge," "considerable skill," or "basic understanding") and other proficiency level indicators should not be included in the Competency description. By omitting these, Competency Areas can be used for multiple proficiency levels.[7]

3. **Associated TKS Statements:** Each Competency Area will be associated with a defined group of NICE Framework Task, Knowledge, and Skill statements that provide a more detailed view of the Competency Area. Note that individual statements may be associated with more than one Competency Area.

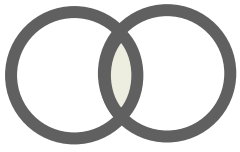
4. Example Uses

The NICE Framework enables rapid adaptation to change while accounting for organizations' unique operating contexts. At the same time, by establishing common language and approach, a consistent exchange of cybersecurity workforce information is possible across an organization, among multiple organizations, and sector wide. The Competency Areas extend the NICE Framework's attributes of agility, flexibility, interoperability, and modularity, which is reflected in the multiple ways that they could be applied by its various stakeholders. There's no one-size-fits-all; they can be used in a variety of ways, including:

- **Overlaid on Work Role(s):** Additional capabilities may be necessary to effectively fulfill one or more Work Roles. A position responsible for more than one Work Role may need the Competency Area across those roles. Example: Cloud Cybersecurity.



- **Common Ground:** A Competency Area can define unique cybersecurity capabilities needed by cybersecurity practitioners and other organizational staff to mitigate risks. In these cases, it serves as a common ground for communication and



[7] NICE also intends to develop a proficiency scale to be used with Competency Areas and Work Roles, per a recommendation of the 2022 report, *Measuring Cybersecurity Workforce Capabilities: Defining a Proficiency Scale for the NICE Framework*.

coordination. Example: Operational Technology (OT) Cybersecurity.

- **Learning:** For students, job seekers, or employees, Competency Areas can serve as a starting place for learning or a way to develop higher-level expertise in an area. Example: Secure Programming.

4.1. Employer Perspective

From an employer perspective, NICE Framework Competency Areas can be used to support workforce hiring, development, and assessment in multiple ways, including to :

- **Describe a given job**: Specific Competency Areas can be used when developing a job description or when defining a new role in an organization.
- **Track workforce capabilities**: Competency Areas can be used to broadly describe and track an organization's cybersecurity workforce capabilities, or an employer might look at a grouping of Task, Knowledge, and Skills and define a custom Competency Area for their unique needs.
- **Specify team requirements**: At times, a team needs to be formed before the individual tasks the team will complete are defined. In these cases, knowing the broader Competency Areas needed by the team to solve the challenge can help identify team members, who will then determine the specific work to be done.
- **Assess individual learner capabilities**: Learners can be assessed against Competency Areas at various or multiple stages, including as part of an interview, a work-based learning evaluation, a promotion process, or career development.

4.2. Education, Training, or Credential Provider Perspective

From an education, training, or credential provider perspective, NICE Framework Competency Areas can similarly be used to support multiple processes, including to:

- **Develop programs**: Providers can use a set of Competency Areas to develop a learning program—bundling together related areas—or to differentiate levels of proficiency within an individual Competency Area.
- **Develop courses**: Instructors might select specific Knowledge and Skill statements in a Competency Area to emphasize those statements in the learning process.
- **Assess students**: Providers can gauge whether a learner has achieved a defined degree of capability in a Competency Area before awarding a credential.

4.3. Learner Perspective

Finally, from the learner's perspective, NICE Framework Competency Areas can be used at various stages and in various ways, including to:

- **Assess one's capabilities**: For example, to determine one's overall capability in a defined Competency Area.
- **Identify areas that may need development**: This can be done through assessment or by using the Competency Area to self-identify areas that require further learning.
- **Learn about a defined area of expertise**: Competency Areas can offer a bird's-eye view for anyone interested in cybersecurity to help them understand needed expertise that may be outside of defined Work Roles, as well as to connect a learner with details via the associated TKS statements.
- **Navigate and choose career paths:** Understanding ones' capabilities in defined Competency Areas can help learners to identify and progress towards related Work Roles and jobs.
- **Understand an organization's workforce needs**: For learners who are looking for a new job, in a current job but wanting to make a shift, or are planning their career path, Competency Areas can give insight into an organization's specific cybersecurity workforce needs.

5. List of NICE Framework Competency Areas

NICE Framework resources, including the latest list of Competency Areas, are available in the NICE Framework Resource Center. NIST is maintaining the Competency Areas list separate from this document and from the NICE Framework publication to allow for regular review and updates. The NICE Framework Resource Center also includes information on how to engage in and keep informed on updates and development of the NICE Framework and supporting resources.

References

[1] Petersen R, Santos D, Wetzel K, Smith M, Witte G (2020) Workforce Framework for Cybersecurity (NICE Framework). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1. https://doi.org/10.6028/NIST.SP.800-181r1

[2] National Institute of Standards and Technology (2021) *NICE Framework Resource Center.* Available at https://www.nist.gov/itl/applied-cybersecurity/nice/resources

[3] Berry J (2011) *Competency Model for Cybersecurity*. (U.S. Office of Personnel Management, Washington, DC), U.S. Office of Personnel Management Memorandum, February 16, 2011. Available at https://www.chcoc.gov/content/competency-model-cybersecurity

Appendix A. List of Symbols, Abbreviations, and Acronyms

CIO
Chief Information Officer

ITL
Information Technology Laboratory

KSA
Knowledge, Skill, and Ability statements

NICE
Previously 'National Initiative for Cybersecurity Education', NICE now only goes by its acronym

NIST
National Institute of Standards and Technology

OPM
Office of Personnel Management

TKS
Task, Knowledge, and Skill statements

Appendix B. Glossary

The following identifies terms used in the NICE Framework and presents definitions in that context. For a complete glossary of terminology used in NIST's cybersecurity and privacy standards and guidelines, please visit https://csrc.nist.gov/glossary.

Capability
A person's potential to accomplish something.

Competency Area
A cluster of related Knowledge and Skill statements that correlates with one's capability to perform Tasks in a particular domain. Competency Areas can help learners discover areas of interest, inform career planning and development, identify gaps for knowledge and skills development, and provide a means of assessing or demonstrating a learner's capabilities in the domain.

Knowledge
A retrievable set of concepts within memory.

Learners
Individuals who perform cybersecurity work, including students, job seekers, and employees.

Skill
The capacity to perform an observable action.

Task
An activity that is directed toward the achievement of organizational objectives.

Work Role
A grouping of work for which an individual or team is responsible or accountable.