Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn and is provided solely for historical purposes. It has been followed by the document identified below.

Withdrawal Date	June 21, 2023
Original Release Date	December 15, 2021

The attached draft document is followed by:

Status	Final
Series/Number	NIST Interagency or Internal Report 8355
Title	NICE Framework Competency Areas: Preparing a Job-Ready Workforce
Publication Date	June 2023
DOI	https://doi.org/10.6028/NIST.IR.8355
CSRC URL	https://csrc.nist.gov/publications/detail/nistir/8355/final
Additional Information	NICE Framework Resource Center

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

Draft (2nd) NISTIR 8355

NICE Framework Competencies:

Assessing Learners for Cybersecurity Work

Karen A. Wetzel

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8355-draft2

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

Draft NISTIR 8355

NICE Framework Competencies:

Assessing Learners for Cybersecurity Work

Karen A. Wetzel (Manager of the NICE Framework)
National Initiative for Cybersecurity Education (NICE)
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8355-draft2

December 2021

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

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8355
18 pages (December 2021)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8355-draft2

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: ***December 15, 2021*** **through** ***January 31, 2022***

Email: NICEFramework@nist.gov
National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

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.

Abstract

This publication from the National Initiative for Cybersecurity Education (NICE) describes Competencies as included in the *Workforce Framework for Cybersecurity (NICE Framework)*, NIST Special Publication 800-181, Revision 1, a fundamental reference for describing and sharing information about cybersecurity work. The NICE Framework defines Task, Knowledge, and Skill (TKS) statement building blocks that provide a foundation for learners, including students, job seekers, and employees. Competencies are provided as a means of applying those core building blocks by grouping related TKS statements to form a higher-level statement of competency. This document shares more detail about what Competencies are, including their evolution and development. Additionally, the publication provides example uses from various stakeholder perspectives. Finally, the publication identifies where the NICE Framework list of Competency Areas is published separate from this publication and provides the rationale for why they will be maintained as a more 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.

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 (JP Morgan 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.

Audience

The NICE Framework serves as a bridge between employers and education and training providers as well as a tool to help learners determine needs and demonstrate capabilities. Providing a standardized approach to Competencies provides direct information about what a workforce needs to know, enables the development of more effective learning, and establishes regular processes to consistently describe and validate a learner’s capabilities. Therefore, employers, workforce development and human resources professionals, education and training providers, learners, and others are stakeholders and the audience for this work.

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 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 Reviewers

This draft publication assumes some existing knowledge of the NICE Framework and is expected to be read in that context. This is the second draft of this document. The first draft was released in March 2021 along with an initial list of proposed Competency Areas. Feedback received on that first draft, conversations with NICE community members, and insights from workshops that brought together subject matter experts have matured our understanding of NICE Framework Competencies. The adjustments to this document are the result. In addition, we will be working with community stakeholders to further refine the proposed list of Competency Areas for release in 2022. Any subsequent draft(s) may be further adjusted, including the Competency Areas, their descriptions, and associated Task, Knowledge, and Skill (TKS) statements.

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

1 Introduction

The *Workforce Framework for Cybersecurity (NICE Framework)*, NIST Special Publication 800-181, Revision 1, was released in November 2020 [1]. This revision establishes at the core of the NICE Framework a set of building blocks – Tasks, Knowledge, and Skills – as well as identifies common ways that the Framework can be applied, most notably through Work Roles and, new in this revision, Competencies (see Appendix 1: Evolution of NICE Framework Competencies). The NICE Framework building blocks, Work Roles, and Competencies will be maintained separately and made available as part of the NICE Framework Resource Center in order to allow for regular review and updates [2].

Competencies are a means to apply the NICE Framework core building blocks by grouping related Task, Knowledge, and Skill (TKS) statements to form a higher-level statement of competency. They further provide a means of learner—which, for the purposes of the NICE Framework includes students, job seekers, and employees—assessment by clearly defining what a person needs to know and be able to do to perform well in a defined area of cybersecurity work. They are defined via an employer-driven approach that provides insight to an organization's unique context. Because of this, they also allow education and training providers to be responsive to employer or sector needs by creating learning experiences that help learners develop and demonstrate the Competencies. For the purposes of the NICE Framework, a Competency is a measurable cluster of related Task, Knowledge, or Skill statements in a particular domain that correlates with performance on the job and can be improved through education, training (including on-the-job or via apprenticeships), or other learning experiences.

1.1 Purpose

This publication introduces readers to NICE Framework Competencies and why they were introduced in the revised NICE Framework publication; describes how the Competencies are defined and written; and shares with readers ways NICE Framework Competencies can be used.

1.2 Scope

The Competencies defined in this publication are for use with 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.

2 Competencies and the NICE Framework

The introduction of Competencies into the NICE Framework is a response to a growing need for a skilled cybersecurity workforce. Indeed, private sector employers have already begun shifting to meet needs, including modernizing recruitment practices to better identify and secure talent through skills- and competency-based hiring. Hiring based only on degrees increases the likelihood to exclude qualified candidates, particularly for jobs related to emerging technologies, and 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. The introduction of Competencies into the NICE Framework thereby provides a means of helping the multiple NICE Framework audiences shift in this direction.

Competencies offer flexibility by allowing organizations to group together various Tasks, Knowledge, and Skills (TKS) statements into overarching areas that define a broad need. While an individual Task and its associated Knowledge and Skill statements may not change, a Competency Area may require the introduction of new Tasks or even individual Knowledge and Skills—or remove existing ones—in response to evolving needs in a changing cybersecurity ecosystem. NICE Framework Competencies are complementary to Work Roles and provide a means to assess learner capabilities in the defined areas.

2.1 Evolution of NICE Framework Competencies

NICE Framework Competencies were first introduced in the 2020 revision of that publication but derive from earlier work. The first version of the National Cybersecurity Workforce Framework 1.0 - Interactive PDF (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.[1] 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.[2] 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.[3]

Prior to publishing NIST SP 800-181in 2017, consideration was given as to whether competencies should be maintained in that version. It was determined at that time to not include them in part due to what was felt a need for additional work to provide adequate definitions of the competencies as well as to address inconsistencies with the KSA alignment. When revising

[1] Note that Ability statements were removed in the 2020 revision of the NICE Framework.

[2] 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]

[3] Two categories—"Collect and Operate" and "Analyze"—related to classified content and thus were not included in that alignment review.

the NICE Framework in 2019-2020, inclusion of competencies was revisited and then included in the 2020 publication.

2.2 Defining Competencies

Competencies offer a higher-level perspective on cybersecurity work, allowing organizations to bring together various TKS statements for a defined area of cybersecurity work. As hiring becomes more inclusive of competencies in determining capabilities, applicant pools are broadened to identify candidates more successfully, particularly in areas such as emerging and rapidly evolving technologies. They offer an assessment-based approach to hiring and promotion, in determining career paths, for identifying current gaps and future needs, and in aligning education and training goals. A Competency Area consists of a name, description of the area, and group of associated TKS statements. Importantly, they are:

Competency Area: A measurable cluster of related Task, Knowledge, or Skill (TKS) statements in a particular domain that correlates with performance on the job and can be improved through education, training (including on-the-job and via apprenticeships), or other learning experiences.

Competency Areas consist of a name, description of the area, and group of associated TKS statements.

- Defined via an employer-driven approach
- Learner-focused
- Observable and measurable

Accordingly, instead of specifying the work to be done (Tasks) or what is needed to do the work (Knowledge and Skills), it's about assessing a learner's overall competency for that area of work (the combination of TKS statements that it encompasses). Competencies offer an opportunity to increase alignment and coordination between employers, learners, and education and training providers (see Figure 1: NICE Competencies Stakeholders).

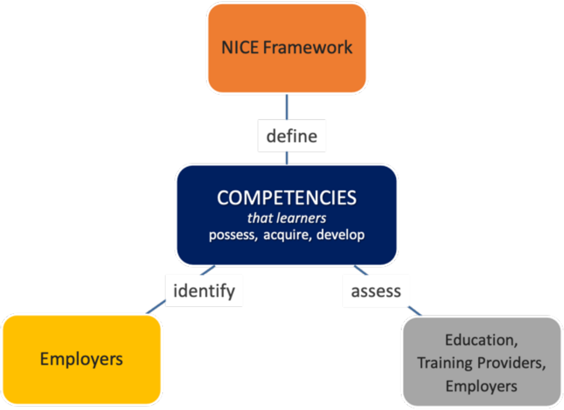

Figure 1: NICE Competencies Stakeholders

NICE Framework Competencies and Work Roles (which identify a group of tasks for which someone is responsible) are complementary and may be used together or separately. However, there are differences. While Competencies are learner-focused, Work Roles are work focused. Competencies help address employer needs, while Work Roles are used when defining positions and responsibilities. Finally, assessment is typically based on the Competency Area as a whole (i.e., Task, Knowledge, and Skills), whereas assessment for Work Roles typically occurs at the Task level.

Competencies

- Learner focused
- Help address employer needs
- Assessment is typically based on a Competency Area as a whole

Work Roles

- Work focused
- Help define positions and responsibilities
- Assessment typically occurs at the Task level

Finally, Competencies are flexible, allowing the inclusion or removal of individual TKS statements in response to shifting needs in a changing cybersecurity ecosystem. As such, a listing of defined NICE Framework Competency Areas will be maintained separate from this publication and made available from the NICE Framework Resource Center as a more flexible and contemporary reference resource.

2.2.1 Developing Competency Statements

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

1. **Competency Area Title:** The name of the competency; the title should clearly signal 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.** Anyone reading the description should be able to quickly and easily understand the scope and meaning of the competency.

   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.

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.

2.2.2 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 Competencies 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 a Work Role. A position responsible for more than one Work Role may need the Competency Area across those roles (e.g., cloud security).
- **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 coordination (e.g., control systems cybersecurity).
- **Learning:** For students, job seekers, or employees, they can serve as a starting place for learning or a way to develop higher-level expertise in an area (e.g., digital forensics).

2.2.2.1 Employer Perspective

From an employer perspective, applications include:

- **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, the Competencies necessary to solve a challenge can be used to identify team members, who will then determine the specific work to be done.

- **Assess individual learner capabilities**: Learners can be assessed against various Competency Areas at various or multiple stages, including as part of an interview, a work-based learning evaluation, a promotion process, or career development.

2.2.2.2 Education, Training, or Credential Provider Perspective

From an education, training, or credential provider perspective, applications include:

- **In program development**: Providers could use a set of Competencies to develop a learning program—bundling together related competencies—or differentiate levels of proficiency within an individual Competency Area.

- **In course development**: Instructors might look at the most important Knowledge and Skill statements reflected in a Competency Area to emphasize those statements in the learning process.

- **In student assessment**: Providers could gauge whether learners have achieved competency in a Competency Area before awarding a credential.

2.2.2.3 Learner Perspective

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

- **Assess one's capabilities**: For example, to determine one's overall competency 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**: Competencies can offer a bird's eye view for anyone interested 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.

- **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, Competencies can give insight into an organization’s specific cybersecurity workforce needs.

References

[1] Petersen R, Santos D, Wetzel K, Smith M, Witte G (2020). (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, 2021. Available at https://www.chcoc.gov/content/competency-model-cybersecurity

Appendix A—Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

CIO	Chief Information Officer
KSA	Knowledge, Skill, and Ability (KSA) statements
NICE	National Initiative for Cybersecurity Education
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.

Competency A measurable cluster of related Task, Knowledge, or Skill (TKS) statements in a particular domain that correlates with performance on the job and can be improved through education, training (including on-the-job and via apprenticeships), or other learning experiences.

Knowledge A retrievable set of concepts within memory.

Skill The capacity to perform an observable action.

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

Work Role A way of describing a grouping of work for which someone is responsible or accountable.