Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date December 15, 2021

Original Release Date March 17, 2021

Superseding Document

Status	2nd Public Draft (2PD)
Series/Number	NIST Interagency or Internal Report 8355
Title	NICE Framework Competencies: Assessing Learners for Cybersecurity Work
Publication Date	December 2021
DOI	https://doi.org/10.6028/NIST.IR.8355-draft2
CSRC URL	https://csrc.nist.gov/publications/detail/nistir/8355/draft
Additional Information	https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

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

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

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-draft

March 2021

U.S. Department of Commerce
Gina 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 (March 2021)

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

Public comment period: *March 17, 2021* through *May 3, 2021*

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

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

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 to apply those core building blocks by grouping related TKS statements for 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 Competencies list 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; cyber; cybersecurity; cyberspace; education; knowledge; risk management; role; security; skill; task; team; training; workforce; work role.

Acknowledgments

The National Institute of Standards and Technology 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. The National Institute of Standards and Technology 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. In addition, it is to be understood that this is an initial draft and that subsequent draft(s) will not only incorporate feedback received from this public comment period but the associated Competencies list will be further defined as Competencies are grouped according to Task, Knowledge, and Skill (TKS) statements.

In addition to comments on the direct contents in this publication, please consider the following:

1) We would like to develop detailed use cases that can be used as implementation models. This document provides some high-level example uses, and it would be helpful to know if these are the primary use cases and what other might exist.

2) It will be important to distinguish uses cases for when NICE Framework Work Roles and Competencies might need to be used separately as well as when they can be used in tandem.

3) The accompanying NICE Framework Competencies list groups the Competencies by type (technical, operational, professional, or leadership). We are seeking to understand whether providing types is valuable and, if so, if the currently identified types meet needs.

4) Currently, the Competencies list includes some identified by the type "professional"—often thought of as employability or soft skills. Moving forward, we are seeking to understand how these important capabilities should be a part of Competencies; for instance, whether they should be:

    a. Included as NICE Framework Competencies, with associated TKS statements.

    b. Included as Knowledge or Skill statements that would be added to NICE Framework Competencies (note that TKS statements in the NICE Framework do not currently reflect professional capabilities).

    c. Not included directly; instead, the NICE Framework should simply reference other resources that provide details about professional capabilities that apply across multiple workforces.

5) Additionally, there are various existing professional skills models in existence, many of which were consulted in the development of the NICE Framework Competencies. Moving forward, we will need to determine if the Competencies should reference a single extant model should be used (and which one) or if multiple models should be assessed to determine which professional capabilities to integrate.

6) The NICE Program office would like to learn more about if and how proficiency levels (e.g., basic, intermediate, and advanced) should be incorporated into NICE Framework Competencies. It will be helpful to identify specific use cases around the use of proficiency levels and Competencies to help us better understand needs in this space, including references to extant models that should be considered in this effort.

7) NICE is in the process of defining a change process for regular updates and input in the NICE Framework components (Competencies, Work Roles, and TKS statements) to allow for adjustments to address, for instance, changes in technology and use. In addition, this process will be used to identify gaps (such as operational technology) that currently exist. Understanding more about gaps and how they can be addressed will be helpful in advance of our planning.

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 way to describe the assessment of a learner by clearly defining what a person needs to know and be able to do to perform well in a job or role. 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 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; shares more about what competencies are and why they were reintroduced in the revised NICE Framework publication; describes how the Competencies were defined and written; and gives readers more information on how the NICE Framework can be used from a Competencies perspective.

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 reintroduction of Competencies into the NICE Framework is a response to a growing need for a skilled cybersecurity workforce. Indeed, private employers have already begun shifting to meet needs, including by modernizing recruitment practices to better identify and secure talent through skills- and competency-based hiring. Degree-based hiring is especially likely to exclude qualified candidates 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 is a means of helping the multiple NICE Framework audiences to shift in this direction.

Competencies offer flexibility by allowing organizations to group together various Tasks, Knowledge, and Skills (TKS) statements into an overarching groups that defines a broad need. While an individual Task and its associated Knowledge and Skill statements may not change, a more broadly defined Competency 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.

The NICE Framework Competencies are a way for organizations to align with the NICE Framework at a high level without necessarily delving into the details of TKS statements, although the associated statements are available and can be referred to if desired. Competencies enable organizations to succinctly communicate and effectively organize their cybersecurity work in order to provide a streamlined view of the workforce.

2.1 Evolution of NICE Framework Competencies

The Competencies set forth in the 2020 NICE Framework publication 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. Following subject matter expert panel review of the OPM model, 50 competencies were found to be aligned with the NICE Framework KSAs found in five of the seven categories of work.[3]

[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

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.

2.2 Defining Competencies

Ultimately, the NICE Framework defines Competencies as a mechanism for organizations (including employers as well as education and training organizations) to assess learners. Competencies consist of a name, description of the Competency, and group of associated TKS statements. Importantly, they are:

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

Competency: A mechanism for organizations to assess learners. Competencies consist of a name, description of the Competency, and group of associated TKS (Task, Knowledge, Skill) statements.

Competencies are:
- 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 ability to do that 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).

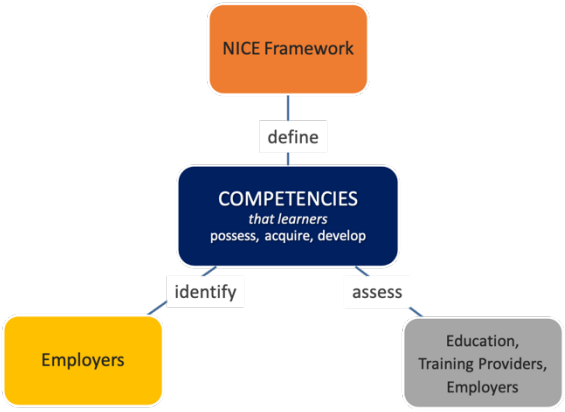

Figure 1: NICE Competencies Stakeholders

Competencies offer a higher-level perspective on cybersecurity work, allowing organizations to bring together various TKS statements into an overarching group that defines a broad need. As such, they allow organizations to, for instance, develop position descriptions without having to

alignment review.

delve into the details of the statements they comprise. In addition, Competencies are flexible, allowing the inclusion or removal of individual TKS statements over time in response to shifting needs in a changing cybersecurity ecosystem. It is recognized that additional work is required to review and update existing TKS statements in order to better align them to the identified list of competencies. That work is ongoing and will be updated periodically.

2.2.1 Developing Competency Statements

The following guidelines are used for the development of Competencies as part of the NICE Framework.

1. **Competency Title:** The name of the competency; the title should clearly signal to all stakeholders the area that will be described.

2. **Competency Description:** The description should:

    a. **Begin with "This Competency 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 description while focusing the competency onto the learner (as opposed, for instance, to a Work Role or Task) at the onset.

    b. **Define the Competency 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, though it should not wholly duplicate that language.

    d. **Balance specificity with broad application.** A goal of a NICE Framework Competency 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 indications of proficiency level should not be included in the Competency description.

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

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 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 with a variety of assessment methods and, because of the way that Competencies tie in with the core NICE Framework building blocks, they can be used in parts or as a whole.

NICE Competencies provide users with a basis for building integrated human resource management systems that use a common set of Competencies to structure job design, recruitment, selection, performance management, training, and career development so that employees receive a consistent message about the factors on which they are selected, trained, and evaluated.

2.2.2.1 Employer Perspective

From an employer perspective, some ways Competencies can be used to:

- **Describe a given position**: For instance, position descriptions can refer to defined Competencies when developing a job description or defining a new role for their organization.

- **Track workforce capabilities**: Defined Competencies can be used to broadly describe and track an organization's cybersecurity workforce knowledge and skills, or an employer might look at a grouping of tasks and define a Competency from that group for their unique needs.

- **Specify team requirements**: At times, individual tasks a team might need to complete may be unknown at the onset. In these cases, the Competencies necessary to solve the 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 Competencies 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, some applications might include:

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

- **In course development**: Instructors might look at the most important Knowledge and Skill statements reflected in a Competency to focus on teaching those.

- **In student assessment**: Providers could use Tasks in a Competency to assess whether learners have achieved the knowledge and skills needed in that area in order to issue 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, such as to:

- **Assess one's abilities**: For example, to determine if one can complete defined tasks in a Competency.

- **Identify areas that may need development**: This can be done through assessment or by using the Competency 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 discover more defined areas, as well as connect a learner to the details via the associated TKS statements.

- **Understand an organization's workforce needs**: For learners who are looking for a new job, in a current position but may want to make a shift, or want to plan their career path, Competencies can give insight into an organization's cybersecurity workforce.

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. (The White House, Washington, DC), U.S. Office of Personnel Management Memorandum, February 16, 2011. 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 mechanism for organizations to assess learners.
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.