NICE Framework Competency Areas: Introduction and Proposed List

June 21, 2023

Comment Period: June 21 – August 5, 2023

How to Review and Submit Comments

1. Review this introduction and the proposed list of NICE Framework Competency Areas.
2. Send Comments to NICEFramework@nist.gov no later than August 5, 2023, at 11:59 p.m. ET.

Feedback received during this comment period will be used to inform any necessary updates to the proposed Competency Areas. Comments will be reviewed and adjudicated, and changes may be made based on feedback. Once the NICE Framework Competency Areas are confirmed, NICE will work with stakeholders and subject matter experts to identify existing and develop new statements to assign to the determined Competency Areas.

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

Table of Contents

Introduction

In response to an upsurge in the use of skills- and competency-based recruitment and hiring among employers, Competency Areas were added to the NICE Workforce Framework for Cybersecurity (NICE Framework), NIST SP 800-181 Rev.1, in 2020. Identifying talent based only on degrees or other credentials has the potential to exclude qualified candidates, particularly for jobs related to emerging technologies, compounding the challenge of meeting the rapidly expanding workforce demand. Providing a standardized approach to Competency Areas 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. The audience for this work includes employers, workforce development and human resources professionals, education and training providers, learners, and others.

Following the 2020 NICE Framework revision, NICE released an initial draft list of competencies for comment in May 2021. This document summarizes the second draft of the proposed list of Competency Areas, providing insights into the information received during the initial list's comment period and from additional stakeholder conversations held subsequent to that call.

Note that two related publications are now available and may provide additional insights into the NICE Framework Competency Areas:

- NICE Framework Competency Areas: Preparing a Job-Ready Cybersecurity Workforce (NISTIR 8355): This document was released as a draft twice for comments prior to its final publication in 2023.[1] Competency Areas are a part of the NICE Framework; the NISTIR is supplemental content that provides a high-level overview of NICE Framework Competency Areas and how they may be used as part of the NICE Framework.
- Competency Areas Authoring Guide for Workforce Frameworks: This draft document supports the creation of Competency Areas in workforce frameworks, similar to the previously released Task, Knowledge, Skill (TKS) Statements Authoring Guide for Workforce Frameworks. It serves as a guide in the development of the Competency Areas and is being made available as part of the Playbook for Workforce Frameworks.

Developing the Proposed Competency Areas List

The inclusion of Competency Areas in the first revision of SP 800-181 builds on work going back to a coordinated effort with the Federal Chief Information Officers (CIO) Council and NICE in November 2009 that informed the 2011 U.S. Office of Personnel Management (OPM) memorandum introducing a "Competency Model for Cybersecurity."[2] In March 2021 a draft list of 54 proposed NICE Framework

[1] The first draft of NISTIR 8355 was released for comment on March 17, 2021 (https://www.nist.gov/news-events/news/2021/03/nice-framework-competencies-assessing-learners-cybersecurity-work); the second draft was released December 15, 2021 (https://www.nist.gov/news-events/news/2021/12/public-comment-invited-draft-nice-framework-update-process-refactored). The final publication was made available June 2023 and is available at: https://doi.org/10.6028/NIST.IR.8355

[2] United States Office of Personnel Management (16 February 2011). "Competency Model for Cybersecurity" [Memorandum]. https://www.chcoc.gov/content/competency-model-cybersecurity

competencies that largely derived from the 2011 OPM was released for comment.[3] The 2021 list included a name and short description for each competency and sorted them into one of four categories. Submitted feedback specific to the proposed list identified the following issues:

- Competency categories (organizational, professional, leadership, and technical): Although some comments indicated that the categories were helpful in showing the breadth of cybersecurity work, most comments on the categories were not favorable. Many noted that competencies could frequently fit into multiple categories, so sorting each one into a single category was problematic. Additionally, many commenters indicated that it was unclear what purpose the categories served, and it was largely recommended that they be removed.
- Professional competencies: Commenters generally agreed on the importance of professional skills (often known by a variety of terms, such as soft skills, employability skills, human skills, or foundational skills) for the cybersecurity profession. However, there was broad consensus that they should be considered skills, not competencies, and that NICE should not identify these as part of the NICE Framework. Several comments also acknowledged existing frameworks that focused on professional skills as potential alternative sources for this content.
- Competencies vs. Work Roles: Comments made clear that there needed to be a greater distinction between the competencies and NICE Framework Work Roles, as well as additional clarification regarding how these two would work together. The comments also identified redundancy between the proposed list and the NICE Framework Work Roles and noted this redundancy as problematic.

As a result of this feedback, the NICE Program Office conducted a thorough reexamination of this work. This was informed by changes that were made (based on feedback) to the term "competencies" and its definition, so that what is now proposed are NICE Framework "Competency Areas." This change of language more accurately represents this content as a grouping of knowledge and skill statements into a broader domain that can serve to evidence a learner's capability in that area, versus the term "competency," which is frequently used as a shortcut for one's ability to complete a narrow task.

NICE Framework 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.

– Definition from NICE Framework Competency Areas: Preparing a Job-Ready Cybersecurity Workforce *(NISTIR 8355)*

[3] "NICE Framework Competencies: Assessing Learners for Cybersecurity Work" (March 17, 2021). Available at: https://www.nist.gov/news-events/news/2021/03/nice-framework-competencies-assessing-learners-cybersecurity-wor

Additionally, a study of how the Competency Areas relate to Work Roles was also made, resulting in the following principles:

- Competency Areas may:
  - Be additive to one or more Work Roles
  - Span multiple Work Roles
  - Represent emerging domains
- Competency Areas do not duplicate Work Roles

The reexamination included comparison of the originally released draft list against the following:

- Recommended New Competency Areas: Some commenters on the first draft list proposed new areas for inclusion. These were reviewed and considered as part of the second draft process.
- NICE Framework Work Roles and TKS Statements: A review of the initial draft list compared to NICE Framework Work Roles and their associated TKS statements was conducted to identify duplication and redundancies. Areas that were found to be significantly redundant were excluded.
- NICE Framework Specialty Areas: Although Specialty Areas were deprecated in the NICE Framework 2020 revision, a comparison of the first draft list of competencies to the 2017 NICE Framework Specialty Areas was made to determine if any of the Specialty Areas might identify capabilities that were not effectively represented by Work Roles and that would be well served as Competency Areas.
- Related Frameworks or Publications: This review aimed to identify whether related frameworks identified areas that were not sufficiently represented by NICE Framework Work Roles and that would be well served as Competency Areas, as well as to determine those areas most frequently addressed by related frameworks and the terminology used to represent those areas. Examples of related frameworks included NIST frameworks or publications (e.g., NIST Cybersecurity Framework[4]), external cybersecurity skills frameworks (e.g., CyBOK[5]), and Knowledge Units for the National Centers of Academic Excellence in Cybersecurity.[6]
- NIST Computer Security Resource Center (CSRC) List of Project Areas: The CSRC project list[7] was consulted to identify emerging areas of cybersecurity research that should be considered as part of the Competency Area review.
- Cybersecurity Certification and Credentialing Sources: A thorough analysis of cybersecurity certification topic areas was conducted in order to determine those areas most regularly identified by the various organizations and the language used to describe those areas.

[4] NIST Cybersecurity Framework. https://www.nist.gov/cyberframework
[5] CyBOK. https://www.cybok.org/
[6] National Centers of Academic Excellence in Cybersecurity. https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/
[7] NIST Computer Security Resource Center Projects. https://csrc.nist.gov/Projects/

In addition to the above, changes to the 2021 draft competencies list in the following areas were made based on community feedback:

- Professional and Non-cybersecurity Specific Skills: In addition to the items that were already included in the "Professional" category, items from the initial draft competencies list that were similar to professional skills or non-cybersecurity specific were also removed (e.g., "Technology Fluency," "Business Acumen," and "Mathematical Reasoning"). Integration of these essential skills will be revisited as part of future work on defining a proficiency scale for use with NICE Framework Work Roles and Competency Areas.[8]
- New Work Roles: The first draft list was also reviewed to determine if it included any items that would be better proposed as new Work Roles. A NICE Framework Work Role comprises a group of Task statements that identify work for which someone or a team is responsible. Work Roles represent areas of work that are well established in cybersecurity and that may exist in various sectors and organization types. For example, "Contracting and Procurement" was identified in this process and will be proposed separately as a new future Work Role.

Following these thorough reviews and analyses, and in consultation with stakeholders, fifteen Competency Areas were identified and are being proposed (provided below). This list is intended to represent highly sought-after Competency Areas that pertain broadly to a variety of industries, sectors, and types of organizations. They represent:

- Fundamental areas of capability needed in cybersecurity,
- Emerging areas that are not yet established enough to be considered Work Roles, and
- Unique domains that may at times be additive to existing Work Roles or represent capability that is needed in multiple Work Roles.

This list is not intended to be exhaustive. Additional Competency Areas may be added over time, while others may be retired or adjusted. NICE will continue to embrace a consultative, open, and transparent approach in its ongoing development.

[8] See *Measuring Cybersecurity Workforce Capabilities: Defining a Proficiency Scale for the NICE Framework*. This report discusses proficiency levels broadly to provide overall context and clarity, points to various extant models, summarizes findings regarding existing efforts to assess proficiency in the workforces of both the public and private sector, and provides recommendations for effective methods for measuring the cybersecurity proficiency of learners. A draft NICE Framework proficiency scale is expected to be released for comment in summer 2023.

NICE Framework Proposed Competency Areas List

The below list identifies only the 15 proposed Competency Area names and descriptions. Once community feedback is received and a final list is confirmed, NICE will engage with the community to determine what—if any—existing NICE Framework statements should be associated with each Competency Area and what new statements may need to be developed.

Proposed Competency Name	Proposed Competency Description
Access Controls	This Competency describes a learner's capabilities to define, manage, and monitor the roles and secure access privileges of who is authorized to access protected data and resources.
AI Security	This Competency describes a learner's capabilities to utilize Artificial Intelligence (AI) to improve cybersecurity.
Asset Management	This Competency describes a learner's capabilities to conduct and maintain an accurate inventory of all digital assets, to include identifying, developing, operating, maintaining, upgrading, and disposing of assets.
Cloud Security	This Competency describes a learner's capabilities to protect cloud data, applications, and infrastructure from threats.
Communications Security	This Competency describes a learner's capabilities to secure the transmissions, broadcasting, switching, control, and operation of communications and related network infrastructures.
Cryptography	This Competency describes a learner's capabilities to transform data using cryptographic processes to ensure it can only be read by the person who is authorized to access it.
Cybersecurity Fundamentals	This Competency describes a learner's capabilities to understand and demonstrate the fundamentals of cybersecurity, including risk management; privacy principles; policy, law, and ethics; networking and systems; digital resilience; digital literacy; and computational literacy.

Proposed Competency Name	Proposed Competency Description
Cybersecurity Leadership	This Competency describes a learner's capabilities to provide leadership and strategic direction to an organization's cybersecurity program.
Data Security	This Competency describes a learner's capabilities to protect data and information systems by ensuring their confidentiality, integrity, and availability.
DevSecOps	This Competency describes a learner's capabilities to integrate security as a shared responsibility throughout the development, security, and operations (DevSecOps) life cycle of technologies.
Cyber Resiliency	This Competency describes a learner's capability related to architecting, designing, developing, implementing, maintaining, and sustaining the trustworthiness of systems that use or are enabled by cyber resources to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks.
OS Security	This Competency describes a learner's capabilities to install, administer, troubleshoot, backup, and conduct recovery of Operating Systems (OS), including in simulated environments.
OT Security	This Competency describes a learner's capabilities to improve and maintain the security of Operational Technology (OT) systems while addressing their unique performance, reliability, and safety requirements.
Secure Programming	This Competency describes a learner's capabilities to create secure code and scripts and assess programming security to enable a system to perform specific functions.
Supply Chain Security	This Competency describes a learner's capabilities to analyze and control digital and physical risks presented by technology products or services purchased from parties outside your organization.