NICE Framework Work Role Categories and Work Roles: An Introduction and Summary of Proposed Updates

April 17, 2023

Comment Period: April 17 - June 23, 2023

Review the spreadsheet of proposed updates and submit comments by email to NICEFramework@nist.gov.

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

Table of Contents

1 Introduction

In November 2020, the National Initiative for Cybersecurity Education (NICE) at the National Institute of Standards and Technology (NIST) released the first revision of the Workforce Framework for Cybersecurity (NICE Framework) (NIST SP 800-181r1). This published document updates the 2017 NICE Cybersecurity Workforce Framework (NIST SP 800-181), which was based largely on previous federal initiatives that extend back to at least September 2012, codifying existing practices drawn from multiple federal government departments and agencies.

Through wide-ranging development and use, the NICE Framework has evolved into a national framework that is applied across government at all levels, in the private sector, and in education and training. Since the 2017 publication was released, NICE has received extensive input from these national stakeholders as they have used the NICE Framework to describe and share information about cybersecurity work. That input directly led to the changes that were incorporated in the 2020 revision, the most significant of which are:

- Deprecation of Specialty Areas
- Deprecation of Ability Statements
- Addition of Competency Areas
- Shifting of NICE Framework data (Competency Areas, Work Roles, and Task, Knowledge, and Skill (TKS) statements) to live outside the 800-181 PDF document

These changes work together to ensure that the NICE Framework remains agile, flexible, modular, and interoperable. Cybersecurity is not a field where the work remains static—it is ever-evolving and, to help establish an effective and capable cybersecurity workforce, the NICE Framework content also must be adjustable to meet current needs. The necessary adjustments ensure that the content will continue to accurately describe the cybersecurity workforce, with the right balance of simplicity and complexity to be truly useful to all stakeholders. To achieve these goals, the 2020 revision focuses on defining core building blocks—the Task, Knowledge, and Skill (TKS) statements—and provides multiple ways these can be applied: via teams, Work Roles, and Competency Areas.

NICE is pleased to continue to refine and clarify this fundamental reference resource with the proposed updates to Work Role Categories and Work Roles outlined below. The proposed adjustments are based on feedback from the community during previous calls for comments, during regular engagement with stakeholders, and through consultations with subject matter experts. The draft changes focus on:

- Work Role Categories: Minor updates to Category names, descriptions, and ordering.
- Work Roles: Updates to names, minor updates to descriptions, and new IDs.

Additionally, some shifting of Work Roles is proposed, both within Categories and, in just a few cases, between Categories. One Category and two Work Roles are eliminated in this draft. **Details and tables highlighting the changes are provided below, and a separate spreadsheet of the proposed updates is available at: https://www.nist.gov/document/nice-framework-work-role-proposed-updates-april-2023.**

The process of refining and clarifying Work Roles is iterative. NICE anticipates that after these initial updates are finalized, a review of the statements associated with each Work Role will be necessary to ensure that they accurately reflect the work for which the role is responsible. NIST enjoys a long-standing tradition of transparency, and the NICE Program Office will be highly communicative of the proposed adjustments as we continue to improve the usability of the NICE Framework statements. As is consistent with NIST and NICE practices, future work will also continue to engage practitioners throughout and offer public comment periods to ensure a wide range of stakeholder input in these efforts.

We welcome your feedback as we continue to improve and enhance the usefulness of the NICE Framework.

2 Summary of Proposed Updates

This summary discusses the proposed updates, beginning with the Work Role Categories followed by the Work Roles themselves.

2.1 Work Role Category Updates

Proposed updates to Work Role Categories address Category names, Category descriptions, and the order in which the Categories appear when referenced by the NICE Framework. One Category would be eliminated and its corresponding Work Roles shifted to other Categories.

2.1.1 Category Names

Updates to Work Role Category names and descriptions are proposed for clarity, consistency, and accuracy. (See Table 1 below.)

- **Category Name Adjustments** (see *Section 2.1.4 Category Descriptions* for corresponding description updates)
  Proposed name adjustments include:
  - Changing *Securely Provision* to *Design and Development* (DD) to better reflect the Work Roles in this Category.
  - Changing *Operate and Maintain* to *Implementation and Operation* (IO) to better reflect the Work Roles in this Category.
  - Changing *Analyze* to *Intelligence* (IN) to correspond with the Department of Defense Cyber Workforce Framework (DCWF) naming language for this Category.[1]
  - Changing *Collect and Operate* to *Cyberspace Effects* (CE) to correspond with the DCWF naming language for this Category.[2]
  - Two additional Category names are converted to nouns rather than verbs to be consistent with naming changes for the *Analyze* and *Collect and Operate* Categories (see above): *Oversee and Govern* (OV) becomes *Oversight and Governance* (OG) and *Protect and Defend* (PR) becomes *Protection and Defense* (PD) and
- **New Two-Letter Abbreviations**
  Proposed abbreviations use the first letter of each key word of a Category or the first two letters in the case of one-word Categories.

2.1.2 Category Elimination

Under this proposal, the Category Investigate is eliminated, and its three Work Roles (*Cyber Crime Investigator*, *Law Enforcement/Counterintelligence Forensics Analyst*, and *Cyber Defense Forensics Analyst*) are transferred to Protection and Defense (PD). This change is proposed based on subject

[1] Department of Defense Cyber Workforce Framework (DCWF): https://public.cyber.mil/wid/dcwf/

[2] Ibid

matter expert recommendations and brings forensics closer to incident response. (See also *Section 2.2.3 Work Role Mergers*.)

2.1.3 Category Reordering

The proposed Category reordering uses a sequential lifecycle organizational approach, beginning with Oversight and Governance (OG), as shown below in *Table 1: Proposed Work Role Categories*.

Table 1: Proposed Work Role Categories

NICE FRAMEWORK WORK ROLE CATEGORIES	
2017 CATEGORIES AND ABBREVIATIONS	PROPOSED CATEGORIES AND ABBREVIATIONS
Oversee and Govern (OV)	Oversight and Governance (OG)
Securely Provision (SP)	Design and Development (DD)
Operate and Maintain (OM)	Implementation and Operation (IO)
Protect and Defend (PR)	Protection and Defense (PD)
Analyze (AN)	Intelligence (IN)
Collect and Operate (CO)	Cyberspace Effects (CE)
Investigate (IN)	*Eliminated*

2.1.4 Category Descriptions

Proposed updates to Category descriptions improve consistency and reflect changes to Category names and their corresponding Work Roles. (See *Table 2: Proposed Work Role Category Descriptions* below.) Updates include:

- Replacing the terms “IT” and “information technology” with “technology” to reflect the broader environment of cybersecurity work, including operational technology.
- Replacing “or” with “and” when discussing the various activities reflected in a Category.
- Adding the word “national” for the *Cyberspace Effects (CE)* and *Intelligence (IN)* Categories to reflect the fact that they comprise Work Roles authorized by Titles 10 and 50 of the U.S. Code.[3]

[3] Office of the Law Revision Counsel of the United States House of Representatives, “United States Code.” Available from: https://uscode.house.gov/browse.xhtml

Table 2: Proposed Work Role Category Descriptions

NICE FRAMEWORK WORK ROLE CATEGORIES		
PROPOSED CATEGORY NAME	**2017 DESCRIPTION**	**PROPOSED DESCRIPTION**
Oversight and Governance (OG)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.	Provides leadership, management, direction, and advocacy so the organization may effectively manage cybersecurity-related risks to the enterprise and conduct cybersecurity work.
Design and Development (DD)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.	Conducts research, conceptualizes, designs, and develops secure technology systems and networks.
Implementation and Operation (IO)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.	Provides the implementation, support, administration, and maintenance necessary to ensure effective and efficient technology system performance and security.
Protection and Defense (PD)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.	Protects against, identifies, and analyzes risks to technology systems or networks. Includes investigation of cybersecurity events or crimes related to technology systems and networks.
Intelligence (IN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.	Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for national intelligence.
Cyberspace Effects (CE)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.	Plans, supports, and executes cybersecurity for cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.

2.2 Work Role Updates

2.2.1 Work Role Names

To improve clarity, consistency, and accuracy, proposed updates to Work Roles names include (for a full list of the proposed name updates, please view the spreadsheet of proposed updates):

- Adjusting title indicators—such as “manager” or “specialist"—to minimize confusion and to avoid being mistaken for job titles. For example, *Enterprise Architect* becomes *Enterprise Architecture*.

- Replacing the terms “IT” and “information technology” with “technology” to reflect the broader environment of cybersecurity work, including operational technology.
- Removing the terms “cyber” and “cybersecurity” from all but three Work Role names, as all the Work Roles are written in the context of the NICE Workforce Framework for Cybersecurity. There are three exceptions where common usage dictates retention: *Defensive Cybersecurity*, *Cyber Operations*, and *Cyber Operations Planning*.
- Adjusting the following Work Role names to better reflect standard language for the roles across and beyond the federal government:
  - *Cyber Defense Analyst* becomes *Cyberspace Defense*.
  - *Cyber Defense Forensics Analyst* becomes *Digital Forensics. (*Note that *Digital Forensics* represents a merging of *Law Enforcement/Counterintelligence Forensics Analysis* and *Cyber Defense Forensics Analysis*. See also *Section 2.2.3 Work Role Mergers*.)
  - *Cyber Operator* becomes *Cyber Operations.*
  - *Information Systems Security Manager* becomes *Systems Management*.
  - *Information Systems Security Developer* becomes *Systems Development*. Note that *Systems Development* represents a merging of *Information Systems Security Developer* and *Systems Developer*. (See also Section 2.2.3 Work Role Deprecations.)
  - *Product Support Manager* becomes *Product Support* and is updated based on language from *DOD Instruction 5000.91: Product Support Management for the Adaptive Acquisition Framework*.[4]
  - *Partner Integration Planner* becomes *Partner Integration*.

2.2.2 Work Role Descriptions

To improve clarity and consistency, proposed updates to Work Role descriptions include:

- Beginning each description with the phrase “Responsible for” to depict a grouping of work rather than an individual’s job or position—a single job may consist of more than one Work Role.
- Replacing the terms “IT” and “information technology” with “technology” to reflect the broader environment of cybersecurity work, including operational technology.
- Removing the terms “cyber” and “cybersecurity” from all but three Work Role descriptions, as all Work Roles are described in the context of the NICE Workforce Framework for Cybersecurity. There are three exceptions where common usage dictates retention: *Defensive Cybersecurity*, *Cyber Operations*, and *Cyber Operations Planning*.

2.2.3 Work Role Deprecations

It is proposed that two Work Roles, *Systems Developer* and *Law Enforcement/Counterintelligence Forensics Analyst,* be deprecated because of significant overlap with other Work Roles. In both cases, the content from these roles is retained and merged into the following updated Work Roles.

- **Systems Development**
  To eliminate significant overlap and reflect standard language for the role across and beyond the federal government, content from *Systems Developer* is merged into *Information Systems Security Developer* to create the updated *Systems Development* Work Role*.* The original

[4] Office of the Under Secretary of Defense for Acquisition and Sustainment, DOD Instruction 5000.91: Product Support Management for the Adaptive Acquisition Framework (November 4, 2021). Retrieved from: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500091p.PDF

descriptions for both Work Roles are nearly identical (with only a single word difference), and the associated statements are redundant. Reviewing the Task statements included in *Systems Developer* but not in *Information Systems Security Developer* (14 in total), it is proposed that these Tasks would also pertain to the *Information Systems Security Developer* role and should therefore be added to the Tasks in that role for this merger, as well as the unique Knowledge and Skill statements found in *Systems Developer* (only 10 out of 80 statements are unique). Statements to be added to *Systems Development*:

- T0067
- T0350
- T0358
- T0378
- T0406
- T0447
- T0464
- T0480
- A0162[5]
- T0488
- T0528
- T0538
- T0558
- T0559
- T0560
- K0207
- K0212
- K0227
- S0018
- S0025
- S0060
- S0097
- S0136
- S0146

- **Digital Forensics and Cybercrime Investigation**
  To eliminate significant overlap, content from the *Law Enforcement/Counterintelligence Forensics Analysis* Work Role is merged into *Cyber Defense Forensics Analysis* to create the updated *Digital Forensics* Work Role. Only five Task statements in *Law Enforcement/Counterintelligence Forensics Analysis* are not found in *Cyber Defense Forensics Analysis*, and three of these five Task statements are found in *Cybercrime Investigation*. It is proposed that:

  - The *Cybercrime Investigation* Work Role description be updated to reference language from the *Law Enforcement/Counterintelligence Forensics Analysis* Work Role.
  - The two Tasks (T0246 and T0439) that are unique to *Law Enforcement/Counterintelligence Forensics Analysis,* plus five Knowledge, Skill, and Ability statements that are found in *Law Enforcement/Counterintelligence Forensics Analysis* but not in *Cyber Defense Forensics Analysis* (K0017, K0107, K0305, S0046, and A0175[6]), will be included in the *Digital Forensics* Work Role.

2.2.4 Work Role Transfers

Proposed updates shift the following Work Roles to different Categories to more accurately reflect the areas of work they fall under:

- *Authorizing Official (*originally *Authorizing Official/Designating Representative)* and *Security Control Assessment (*originally *Security Control Assessor)* shift from Design and Development (originally Securely Provision) to Oversight and Governance (originally Oversee and Govern).

[5] Note that Ability statements have been refactored and will be adjusted accordingly in this merger. For more information, visit: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/workforce-framework-cybersecurity-nice#nfdata

[6] Ibid

- *Threat Analysis* (originally *Threat/Warning Analyst*) shifts from Intelligence (originally Analyze) to Protection and Defense (PD) in recognition that this role is used in both public and private sectors.
- *All-Source Collection Management* (originally *All-Source Collection Manager*), *All-Source Collection Requirements Management* (originally *All-Source Collection Requirements Manager*), and *Intelligence Planning* (originally *Cyber Intel Planner*) shift from Cyberspace Effects (originally Collect and Operate) to Intelligence (originally Analyze) to match the Work Roles in the DCWF category of the same name.
- *Mission Assessment* (originally *Mission Assessment Specialist*), *Exploitation Analysis* (originally *Exploitation Analyst*), *Target Development* (originally *Target Developer*), and *Target Network Analysis* (originally *Target Network Analyst*) shift from Intelligence (originally Analyze) to Cyberspace Effects (originally Collect and Operate) to match the Work Roles in the DCWF category of the same name.

2.2.5 Work Role Reordering

Work Roles are reordered alphabetically within their Work Role Category to improve role findability.

2.2.6 Work Role ID Changes

Under this proposal, the 2017 Work Role IDs are deprecated and replaced with new IDs, as described below in Table 3. These adjustments align the Work Roles to their updated Work Role Categories, and remove references to the deprecated Specialty Areas. Work Role IDs follow the same general structure as previously (two-letter category, three-letter designation, three-digit order) to minimize disruption in tools that use these IDs. Note that the Work Role codes used by the Office of Personnel Management (OPM)[7] are not changed (these are identified in the spreadsheet).

Table 3: Proposed Work Role IDs

2017 ID Structure Example ID: SP-RSK-001 (Authorizing Official/Designating Representative)	**Proposed ID Structure** Example ID: OG-WRL-005 (Authorizing Official)
Two-Letter Category	Two-Letter Category *Updated to reflect new Category names*
Three-Letter Specialty Area	Three-Letter Designation *Specialty Areas were deprecated in the 2020 revision and are replaced here with a designation that identifies the item as a Work Role (WRL)*
Three-Digits *Based on order within the Category*	Three-Digits *Based on new order within the Category*

[7] See the U.S. Office of Personnel Management webpage, "Workforce Planning for the Cybersecurity Workforce," for more information: https://www.opm.gov/policy-data-oversight/human-capital-management/cybersecurity/

3 For More Information

- Proposed Updates to NICE Framework Work Role Categories and Work Roles
- National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity (NICE Framework) (NIST SP 800-181r1)
- NICE Framework Data Reference Spreadsheet (2017 Data)
- NICE Framework Resource Center
- NICE Framework Users Group