NICE Framework Components v2.0.0: Summary of Changes

March 2025

Links:

- NICE Framework Components v2.0.0 (link downloads XSLX file)
- NICE Framework Current Version
- NICE Framework Change Request FAQ
- NICE Framework Change Logs
- NICE Framework Revisions: Update Types, Frequency, and Versioning
- NICE Framework Resource Center

NICE | workforce framework for cybersecurity

Summary of Changes

The March 5, 2025 release of the NICE Framework Components Version 2.0.0 includes the following updates:

- **Work Role Categories:** Removal of two Work Role Categories and the Work Roles contained in them:
  - Cyberspace Effects
  - Cyberspace Intelligence
- **Work Roles:** Two updated and one new:
  - Digital Evidence Analysis (IN-WRL-002) (updated)
  - Insider Threat Analysis (PD-WRL-005) (updated)
  - Operational Technology (OT) Cybersecurity Engineering (DD-WRL-009) (new)
- **Competency Areas:** One updated:
  - Cyber Resiliency (NF-COM-007)
- **Administrative Task, Knowledge, and Skill (TKS) Statement updates:**
  - Fixed typos and spelling errors
  - Removal of duplicate or redundant statements

This release features a new Excel workbook to serve as a reference document for users of the NICE Framework:

> **NICE Framework Components Version 2.0.0**, which replaces the v1.0.0 reference spreadsheet as the authoritative catalog of the NICE Framework Components, includes Work Role Categories, Work Roles, Competency Areas, and Task, Knowledge, and Skill (TKS) statements. A JSON file will be published to accompany the XLSX workbook in the future.

The workbook and additional related information can be found in the NICE Framework Resource Center. Overall, the updates result in the following changes to the number of NICE Framework Components (see Table 1).

Table 1: Comparison Summary of NICE Framework Components Changes

	V 1.0.0	V 2.0.0
Work Role Categories	7	5
Work Roles	52	41
Competency Areas	11	11
TKS Statements (total)	2275	2111
Task Statements	1084	942 (39 New)
Knowledge Statements	640	631 (36 New)
Skill Statements	556	538 (35 New)

More details regarding each of the updated areas are provided below in this document.

Versioning

The NICE Program Office takes a software update versioning approach for NICE Framework Components, with a mix of minor and major updates expected over time. While users of the NICE Framework are always encouraged to reference the most recent published version of the Components, users may choose to continue using older versions. A record of versions and release notes can be found on the NICE Framework History and Change Logs webpage in the NICE Framework Resource Center.

> **This update is considered a Major Update:** *A revision of a specification that breaks backward compatibility with the previous revision of the specification in numerous significant ways.* Systems and tools that use NICE Framework components could be significantly impacted by the removal of the two Work Role Categories and their corresponding contents.

More details regarding update types, frequency, and versioning identifiers can be found in the NICE Framework Resource Center.

TKS Statement Change Types

TKS statements may be retained, added, or withdrawn in an update.

- ***Retained:*** Retained statements use the same identifier (ID) as the previous version of the NICE Framework Components. Retained statements may be unchanged or may include administrative corrections (e.g., spelling or punctuation).

- ***New:*** New statements are marked with an ID not included in the previous version of the NICE Framework Components.

- ***Withdrawn:*** Withdrawn statements are fully removed from the NICE Framework Components. Two types of withdrawn statements exist:
    - **Removed statements:** Statements that have been removed and are not replaced with new statements.
    - **Replaced statements*:*** Replaced statements are withdrawn statements (both the original ID and description) that have been replaced by one or more statements. Replacements happen when:
        - The original statement has been revised and replaced by a new updated statement(s) with a new statement ID(s) (“New”).
        - The original statement is redundant and is replaced by an existing related statement(s) (“Retained”).

      Replacements may be of the same or a different type. For example, a withdrawn Task statement may be replaced with two Task statements and a Knowledge statement. At times, a statement may be both revised and replaced with a new added statement and additionally reference an existing related statement. *Note that no replaced statements appear in v2.0.0 Components.*

Questions regarding this update, suggestions for future changes, and other comments may be sent to NICEFramework@nist.gov.

V 2.0.0 Update Details

Work Role Categories

The release of Version 2.0.0 of the NICE Framework Components includes the removal of two Work Role Categories: Cyberspace Effects and Cyberspace Intelligence. These Categories will continue to be maintained in the Department of Defense (DoD) Cyber Workforce Framework (DCWF).

The roles represented in these two Categories fall under the jurisdiction of the U.S. Code Titles 10 and 50, which relate to military operations and intelligence operations, respectively. DoD Directive 8140.01 establishes the DCWF as the "authoritative reference for the identification, tracking, and reporting of DoD cyberspace positions and foundation for developing enterprise baseline cyberspace workforce qualifications." By contrast, the NICE Workforce Framework for Cybersecurity is intended for broad use across federal, state, local, tribal, and territorial government as well as in the private sector and academia.

In collaboration with our partners at DoD, the NICE Program Office has determined that removing these Categories from the NICE Framework will support improved transparency and alignment with the DCWF.

Table 2: Removed Work Role Categories

Removed Work Role Categories	
CYBERSPACE EFFECTS (CE)	Plans, supports, and executes cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.
CYBERSPACE INTELLIGENCE (CI)	Collects, processes, analyzes, and disseminates information from all sources of intelligence on foreign actors' cyberspace programs, intentions, capabilities, research and development, and operational activities.

Table 3: Removed Cyberspace Effects and Cyberspace Intelligence Work Roles

Work Role Name	Work Role Description	NF ID	OPM ID
Cyberspace Operations	Responsible for gathering evidence on criminal or foreign intelligence entities to mitigate and protect against possible or real-time threats. Conducts collection, processing, and geolocation of systems to exploit, locate, and track targets. Performs network navigation and tactical forensic analysis and executes on-net operations when directed.	CE-WRL-001	321
Cyber Operations Planning	Responsible for developing cybersecurity operations plans; participating in targeting selection, validation, and synchronization; and enabling integration during the execution of cyber actions.	CE-WRL-002	332
Exploitation Analysis	Responsible for identifying access and intelligence collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.	CE-WRL-003	121
Mission Assessment	Responsible for developing assessment plans and performance measures; conducting strategic and operational effectiveness assessments for cyber events; determining whether systems perform as expected; and providing input to the determination of operational effectiveness.	CE-WRL-004	112
Partner Integration Planning	Responsible for advancing cooperation across organizational or national borders between cyber operations partners. Provides guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.	CE-WRL-005	333
Target Analysis	Responsible for conducting target development at the system, component, and entity levels. Builds and maintains electronic target folders to include inputs from environment preparation and/or internal or external intelligence sources. Coordinates with partner target working groups and intelligence community members, and presents candidate targets for vetting and validation. Assesses and reports on damage resulting from the application of military force and coordinates federal support as required.	CE-WRL-006	131
Target Network Analysis	Responsible for conducting advanced analysis of collection and open-source data to ensure target continuity; profiling targets and their activities; and developing techniques to gain target information. Determines how targets communicate, move, operate, and live based on knowledge of target technologies, digital networks, and applications.	CE-WRL-007	132

Work Role Name	Work Role Description	NF ID	OPM ID
All-Source Analysis	Responsible for analyzing data and information from one or multiple sources to conduct preparation of the operational environment, respond to requests for information, and submit intelligence collection and production requirements in support of intelligence planning and operations.	CI-WRL-001	111
All-Source Collection Management	Responsible for identifying intelligence collection authorities and environment; incorporating priority information requirements into intelligence collection management; and developing concepts to meet leadership's intent. Determines capabilities of available intelligence collection assets; constructs and disseminates intelligence collection plans; and monitors execution of intelligence collection tasks to ensure effective execution of collection plans.	CI-WRL-002	311
All-Source Collection Requirements Management	Responsible for evaluating intelligence collection operations and developing effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of intelligence collection requirements. Evaluates performance of intelligence collection assets and operations.	CI-WRL-003	312
Cyber Intelligence Planning	Responsible for developing intelligence plans to satisfy cyber operation requirements. Identifies, validates, and levies requirements for intelligence collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.	CI-WRL-004	331
Multi-Disciplined Language Analysis	Responsible for applying language and cultural expertise with target, threat, and technical knowledge to process, analyze, and disseminate intelligence information derived from language, voice, and/or graphic materials. Creates and maintains language-specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.	CI-WRL-005	151

TKS Statements associated with the removed Work Roles were either *withdrawn and removed* or *retained*. Retained statements were either 1) retained if they exist in other Work Roles or Competency Areas that are included in v 2.0.0 or 2) retained after a NICE Program review of the statements unique to these roles determined the statements could potentially be useful outside of these roles. Statements in this latter grouping are not currently associated with any existing Work Roles or Competency Areas but will be considered for inclusion in future revised or newly added Work Roles or

Competency Areas. Out of the 789 statements associated with the 12 removed Work Roles, 275 were withdrawn.

Additional steps to support increased interoperability and usability between the NICE Framework and the DoD Cyber Workforce Framework are planned; interested stakeholders can keep apprised of the latest NICE Framework resources and releases by joining the NICE Framework Users Group or visiting the NICE Framework Resource Center; learn more at nist.gov/nice/framework.

Work Roles

Outside of the roles mentioned in the above categories, v 2.0.0 of the NICE Framework Components includes the following Work Roles changes. A summary of the roles is available in Table 4; details follow the table.

Table 4: Updated and New Work Roles

Work Role Name	Description	ID	Change Type
Digital Evidence Analysis	Responsible for identifying, collecting, examining, and preserving digital evidence using controlled and documented analytical and investigative techniques.	IN-WRL-002	Revision
Insider Threat Analysis	Responsible for identifying and assessing the capabilities and activities of cybersecurity insider threats; produces findings to help initialize and support law enforcement and counterintelligence activities and investigations.	PD-WRL-005	Revision
Operational Technology (OT) Cybersecurity Engineering	Responsible for working within the engineering department to design and create systems, processes, and procedures that maintain the safety, reliability, controllability, and security of industrial systems in the face of intentional and incidental cyber-related events. Interfaces with Chief Information Security Officer, plant managers, and industrial cybersecurity technicians.	DD-WRL-009	New

- **Digital Evidence Analysis:** This release updates Task, Knowledge, and Skill statements in this Work Role and aligns Knowledge and Skill statements to each Task.

- **Insider Threat Analysis:** This Work Role was initially released with Version 1.0.0 of the NICE Framework Components in March 2024. This update includes minor changes to some Task, Knowledge, and Skill statements and aligns the Knowledge and Skill statements to each Task statement in this role.

- **Operational Technology (OT) Cybersecurity Engineering:** This new Work Role in the NICE Framework Design & Development Work Role Category is the first role in the NICE Framework to focus on operational technology (OT). As with the revised roles above, this release includes an alignment of the Knowledge and Skill statements to each Task statement in this role.

These Work Roles and their updates were developed in coordination and consultation with subject matter experts. Each of these three roles were previously released for public comment and comments received were adjudicated by the NICE Program Office to address any needed changes prior to this release. See the NICE Framework Public Comments page.

Competency Area

Competency Areas were added to the NICE Framework Components with the March 2024 v 1.0.0 release. At that time, only titles, IDs, and descriptions were included. Since that time, the NICE Program Office has been working to develop these areas to include relevant Knowledge and Skill statements. This release includes the first of these updated Competency Areas:

- **Cyber Resiliency Competency Area** (NF-COM-007): This Competency Area describes a learner's capability related to architecting, designing, developing, implementing, and maintaining the trustworthiness of systems that use or are enabled by cyber-related resources in order to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises.

Fifty-six (56) Knowledge statements and sixty-seven (67) skill statements are included in this Competency Area. Of these, twenty-two (22) are new to the NICE Framework.

Administrative Updates

Administrative updates were made for twenty-five (25) TKS statements, as described in Table 5.

Table 5: Administrative Changes

Change Type	Number of Statements
Spelling error fixed	14
Grammar error fixed	1
Duplicate statements removed	6
Minor modifications made for clarity	4

Contact Us

The NICE Program Office welcomes suggestions for improving the usability of these documents. You may make suggestions by email to NICEFramework@nist.gov or by joining the NICE Framework Users Group. Furthermore, the **NICE Framework Resource Center** (nist.gov/nice/framework) includes many more additional resources (e.g., Getting Started, Change Request FAQ, Workplace Skills, Success Stories, etc.) that may be helpful.