NICE | workforce framework for cybersecurity

NICE Framework Component Updates: Releases and Versioning

March 2024

Table of Contents

Introduction

The NICE Program Office at the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce is responsible for maintaining the Workforce Framework for Cybersecurity (NICE Framework). To ensure that the NICE Framework is agile, flexible, modular, and interoperable, it is important that regular reviews and updates can be made to the NICE Framework to respond to and anticipate changes in cybersecurity so that a capable and ready workforce is prepared to mitigate and address ongoing risks. In order to remain effective now and in the future, the NICE Framework components—that is, the underlying Work Role Categories, Work Roles, Competency Areas, and Task, Knowledge, and Skill (TKS) statements — will need to be regularly reviewed and adjusted in order to accommodate changing needs of the cybersecurity workforce. These changes are driven by changing technologies, new threats, and evolving approaches to securing our organizations and our nation. NICE Framework updates are derived from stakeholder feedback received via public comment periods, subject matter expert consultations and events, and community feedback. In the case of the NICE Framework, this means being inclusive of the very broad range of stakeholders that use NIST products—including federal, state, and local governments and tribal territories; private industry; academic, training, and certification organizations; learners (students, job seekers, and employees); tool and platform providers; and international communities.

The 2020 revision of the NICE Framework NIST Special Publication separated the framework structure document from the NICE Framework components themselves. This intentional shift was done to ensure that the data could be more regularly reviewed and maintained (to include updates to existing content, adding in new content, and retiring outdated content)—to expand its usefulness, applicability, and adoption nationwide and internationally by more effectively meeting stakeholder needs and better responding to changes in the cybersecurity workforce landscape.

However, in addition to being responsive, changes also need to be structured and transparent to truly meet stakeholder needs. Updates to NICE Framework components will seek to support the NICE Framework attributes of agility, flexibility, interoperability, and modularity while also offering users a process that will minimize disruption in extant applications of the NICE Framework. The approach to how releases will be made available as defined here is in alignment with NIST’s approach to publication updates, founded on an open public comment model as a means of engaging a wide population in the development process. NIST believes that robust, widely understood, and participatory development processes produce the strongest, most effective, most trusted, and broadly accepted standards and guidelines. The following principles guide NIST's standards and guidelines development:

- *Transparency:* All interested and affected parties have access to essential information regarding standards and guidelines-related activities throughout the development process.

- *Openness:* Participation is open to all interested parties. All stakeholders—including security practitioners, researchers, standards developing organizations, and users—have an opportunity to be meaningfully involved in the standards and guidelines development process.
- *Balance:* NIST solicits input from a wide range of stakeholders representing government, industry, and academia to ensure that its standards are strong, practical, and meet the needs of the Federal Government as well as the broader user community.
- *Integrity:* NIST serves as an impartial technical authority when it is developing standards and guidelines.
- *Technical Merit:* NIST's decisions during the development of standards and guidelines are based on the technical merit of a proposal while being mindful of security, privacy, policy, and business considerations.
- *Global Acceptability:* While the statutory basis for NIST's work in risk management is the need for protection of non-national security federal information systems, NIST standards are the foundation of many information technology products and services that are developed and sold globally.
- *Usability:* NIST aims to develop risk management guidelines that help implementers create secure and useable systems that support business needs and better manage risk for systems and organizations.
- *Continuous Improvement:* NIST strives for ongoing engagement with the cybersecurity and privacy community to continuously improve our standards and guidelines.
- *Innovation:* As a scientific bureau within the U.S. Department of Commerce, NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

This document outlines the types of updates, their planned frequency, and versioning. It is in support of the NICE Strategic Plan, Goal 4, Objective 3: "Establish processes for regularly reviewing, improving, and updating the NICE Framework."

Update Types, Frequency, and Versioning

Updates may be identified internally by NICE Program Office staff or may be proposed by private and public stakeholders, including government, industry, academia, learners, and others at any time. The NICE Program Office will work to achieve consensus on the public and private sector input, balancing the need for both periodic updates based upon emerging needs and the desirability for a stable framework.

Update Types

Updates to NICE Framework components fall into three categories:

1. **Major Updates**: A major update is defined as "A revision of a specification that breaks backward compatibility with the previous revision of the specification in numerous significant ways."[1] For example:
    a. NIST 800-181 Revision 1 (2020) deprecated components of the 2017 NICE Framework (Specialty Areas and Ability statements). Systems and tools that use these components would be impacted significantly.
    b. NIST Framework Components: Refactoring the Ability statements as well as the comprehensive review of TKS statements has resulted in updated statements (including revised, removed, and refactored statements), resulting in a major update to the spreadsheet.
2. **Minor Updates**: A minor update is defined as "A revision of a specification that may add or enhance functionality, fix bugs, and make other changes from the previous revision, but the changes have minimal impact, if any, on backward compatibility."[2]
3. **Administrative Updates**: Errata changes and minor corrections that do not alter the intent of the original.

Frequency of Releases

It is essential that NICE Framework components be regularly reviewed and updated when necessary to reflect employer needs and address changes to the cybersecurity work that learners need to be prepared for. However, it is equally essential that these changes be released in a planned and coordinated fashion so that the community that depends on and leverages the NICE Framework in tools, education and training, hiring, and more is aware of upcoming releases and provided with resources and support to integrate new content and adjust existing content. As such, a planned schedule for releases will be followed, using the following:

- **Major Releases**: A major release of NICE Framework data will occur no more frequently than every three years. Proposed changes to be included in a major release will be announced at least one year prior to final release.
- **Minor Releases**: A minor release of the NICE Framework data will occur no more frequently than once annually. At times updates to be included in a minor release may be made available as a pre-release for use by those who are interested in adopting the content prior to the final release.
- **Administrative Releases**: An errata release of the NICE Framework data may occur at any time and without formal notice.

[1] https://csrc.nist.gov/glossary/term/major_version_update

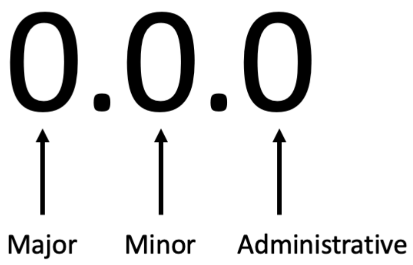
[2] https://csrc.nist.gov/glossary/term/minor_version_update

Note that both major and minor proposed updates will continue to be shared for public comment prior to finalization. The public comment period allows the NICE community to provide feedback on drafts and for the NICE Program Office to incorporate changes and consider the validity of proposed drafts prior to release based on comments received.

NICE Framework releases include all the NICE Framework components. That is, each release will contain the NICE Framework Work Role Categories, Work Roles, Competency Areas, and Task, Knowledge, and Skill (TKS) statements. For example: A new Task statement is being added to the NICE Framework. The release that includes this new statement will comprise all the components, including the statement itself.

Version Identifiers

In order to distinguish between various releases, the following versioning identifier system will be adopted:



Examples

Using 0.0.0 as a starting point, the version will change as follows for the various release types:

- Major Release: 1.0.0 -> 2.0.0
- Minor Release: 1.1.0 -> 1.2.0
- Administrative Release: 1.0.1 -> 1.0.2

These can be combined, as well. For example, following a first major release (1.0.0) there may be several minor releases (1.3.0), followed then by an administrative release (1.3.1). If a major release then followed, that would then reset the second and third place numbers (2.0.0). During the time following a major release and prior to a subsequent major release multiple minor and administrative releases may occur. For example, an administrative release could occur after a major release (e.g., 2.0.1), followed by a minor release (2.1.1), and then a subsequent additional administrative release (2.1.2).

Pre-releases

As noted above, there may be times that data to be included in a minor release may be made available as a pre-release for use by those who are interested in adopting the content prior to the final release. For instance, if a new Work Role is developed, made available for public comment, and then updated based on feedback, that final update may be shared as a pre-release. That way if a second new Work Role or Competency Area is also being readied, the first item can be used while the second is still in development. Then when both are ready, they can be packaged together in the minor release. By doing this, users of the NICE Framework have the option to wait until the minor release so that they can use all the updated minor release content finalized that year, or they can begin using pre-release content if doing so supports their goals. An example of a pre-release draft versioning is:

> 1.1.0d1: In this example, there is a forthcoming minor release (1.1.0) to take place following the initial major release (1.0.0). The content for that minor release (e.g., new Work Role) is being made available early as a draft (draft 1). If additional new content (e.g., a new Competency Area) is also completed and made available for pre-release, the version would change from 1.1.0d1 to 1.1.0d2. Once the minor release is fully released, the version is updated to from 1.0.0 to 1.1.0.

Request for Change Submissions: FAQ

When will I be able to submit requests for changes?
The NICE Framework is developed in coordination with community stakeholders. You can submit updates for consideration:

- **During formal requests for comments.** Stakeholders will be able to view and provide comments on candidates (draft updates available for public comment) during defined comment periods. These time periods are requests for feedback on specific NICE Framework content (e.g., a draft Work Role). Comments on candidates are reviewed by NIST as part of its adjudication process prior to final release of the draft content. Requests for comments are announced on the NICE Framework Resource Center homepage, via the NICE email distribution list, and in other public venues.
- **Outside of comment periods.** Stakeholders can suggest change requests (a "proposal") to the NICE Program Office at any time via NICEFramework@nist.gov. The NICE Program Office may respond to the request immediately for action or may defer the comment for later consideration, e.g., as part of a planned update or during internal quarterly comment review periods. Note that submission of a proposal does not guarantee that NIST will include the proposal in a future comment period (as a "candidate") or release of the NICE Framework.

What is the difference between a Proposal and a Candidate?
Change requests begin as proposals and may advance to candidate status.

- **Proposal:** A proposal is a submitted change request. Proposals may be for new components or for revisions to or withdrawal of existing components.
- **Candidate:** A candidate is a proposal that is available for public comment. Stakeholders will have the ability to review and provide feedback on draft candidates during defined comment periods.

Note that submission of a proposal does not guarantee that NIST will include the proposal in a future comment period (as a "candidate"), and neither proposals nor candidates are guaranteed to be accepted as formal updates.

What kinds of updates can be submitted for consideration?
Changes can be proposed for the following NICE Framework components: Competency Areas, Work Roles and Work Role Categories, and Task, Knowledge, and Skill (TKS) statements. Proposed updates may take the form of:

- **Administrative changes:** These changes address minor administrative errors, including typographical and grammatical errors.
- **Additions:** New statements, Work Roles, or Competency Areas.
- **Adjustments:** Proposals to change existing data elements (e.g., revisions or expansions).
- **Withdrawals:** Proposals to retire existing data elements.

Further, the NICE Program Office will continue to accept suggestions for changes related to the NICE Workforce Framework for Cybersecurity (NICE Framework) (NIST Special Publication 800-181, Revision 1) and NICE Framework Competency Areas: Preparing a Job-Ready Cybersecurity Workforce (NIST Internal Report 8355) as part of future formal requests for comments and informally via the NICEFramework@nist.gov email address.

How will decisions regarding my submission be made?
As a NIST publication, updates to the NICE Framework will be approved by the NICE Program Office after consultation with subject matter experts and stakeholders as needed. These stakeholders may represent government (including federal, state, local, tribal, and territory levels), private industry, academia, training and service providers, and learners (students, job seekers, and employees).

The following will be taken into consideration when reviewing proposed updates:

- How updates align to the Workforce Framework for Cybersecurity (NICE Framework) structure and scope.
- If the proposal is essential and has wide-ranging impact.
- If the proposal addresses workforce needs that apply across sectors, industries, and types of organizations, versus a change to address the unique requirements of an organization or specific industry or sector.
- How the proposal relates to existing NICE Framework content, including the extent of impact an update might make.
- If Task, Knowledge, and Skill (TKS) statement updates adhere to the Task, Knowledge, Skill (TKS) Statements Authoring Guide for Workforce Frameworks.

Proposals received during comment periods are collected and reviewed by the NICE Program Office for adjudication. During this process the NICE staff may reach back out to commenters, subject matter experts, and additional stakeholders for additional information. Adjudication identifies comments as follows:

- **Noted**: Comments that do not require any action (e.g., comments in support of updates).
- **Accepted**: The suggested action provided by the commenter is accepted as is and the update made accordingly.
- **Accepted with Modification**: The feedback provided by the commenter is accepted, though how the update is made may vary from the suggested approach.
- **Deferred**: Typically denote comments that are out of scope of the current comment period but that will be reviewed separately.
- **Rejected**: Feedback that is in scope but that is rejected, typically due to contrary feedback from the community.

Comments received outside of specified comment periods and comments marked as “deferred” from comment periods will be reviewed by NICE Program Office staff to determine if action can be taken. This may include, for instance, incorporating feedback into planned development, informing NICE as to future directions and work, or following up with the commenters or the community on the feedback for further discussion.

How will I know the status of my submission?
Comments received during comment periods receive an acknowledgement of receipt from the NICE Program Office. Following adjudication, adjustments may be made to NICE Framework components based on the feedback received. This updated content is shared with the community (either as updated version or as a subsequent draft for further comment) with a summary of the feedback received during the comment period.

Comments received outside of comment periods as well as deferred comments will be reviewed periodically by NICE staff. Periodic summaries of the comments that have been received and any actions taken by the NICE Program Office will be made available. Items that are marked as “Under Review” during these periods may require additional stakeholder conversation and may also be noted in the summary.

In addition, you can contact the NICE Program Office at any time with specific questions (NICEFramework@nist.gov).

How will I find out about approved updates?
A change log will be maintained and all updates will be communicated via the NICE Framework Resource Center and via the NICE Framework Users Group.

Can I continue to use earlier versions of data?
A detailed change log and unique version identifiers will be used to maintain version control of the NICE Framework components as they evolve (see NICE Framework Revisions for more information). As such, earlier versions of content, including withdrawn content, will still be available for use.

What information should I include in my change request?
Please include the following details in your change request:

1. **Contact Information:** This information will allow us to reach you if there are questions. It will not be shared publicly.
    a. Name
    b. Title
    c. Organization
    d. Email address
2. **Rationale:** An explanation as to why the change is being proposed, including information regarding the proposed change's impact and timeliness.
3. **Type of Change:** Please note what type of change is being proposed:
    a. New Component
    b. Update to Existing Component
    c. Suggested Removal of Existing Component
4. **Proposed Change:** The change itself. This may include not just the core change, but also address how that change may impact other related aspects of the NICE Framework. For instance, a new Task statement should include information regarding which Work Role(s) the Task should be associated with. A new Work Role should include which Work Role Category it would fall under, as well as any information regarding existing or new TKS statements that would be tied to that role. A suggested deletion should discuss whether the deletion would be replaced with updated content, or if it is being proposed as removed only from one area (e.g., a specific Competency Area) or across the NICE Framework.

The NICE Program Office looks forward to ongoing engagement with the community to ensure that the NICE Framework continues to evolve and be a useful resource in support of the cybersecurity workforce. Please visit the NICE Framework Resource Center for ways to engage, to find useful guidance and tools, and to learn about latest updates. We also encourage you to join the NICE Framework Users Group to support the implementation and continuous improvement of the NICE Framework through community collaboration and knowledge-sharing.