NICE Framework Knowledge and Skill Statement Review: An Introduction and Summary of Updates

Comment Period: April 19 – June 3, 2022

Send comments by 11:59 p.m. ET on Friday, June 3, 2022 to: niceframework@nist.gov

National Institute of
Standards and Technology
U.S. Department of Commerce

Introduction

In November 2020, the National Initiative for Cybersecurity Education (NICE), a program in the National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce, 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 largely based upon previous federal initiatives that extend back to at least September 2012, codifying existing practices drawn from multiple federal government departments and agencies. Through extensive development and use, the NICE Framework has evolved into a national framework that is used across government at all levels, in the private sector, and in education and training. In the years 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 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 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 needs to have the ability to adjust to meet current needs. These necessary adjustments ensure the content will continue to accurately describe the cybersecurity workforce, while ensuring that the NICE Framework balances the need to be streamlined enough for application yet offers enough complexity to be truly useful. 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. In early 2021, the Task, Knowledge, Skill (TKS) Statements Authoring Guide for Workforce Frameworks (TKS Authoring Guide), a collaborative NIST effort between NICE and the Privacy Engineering Program (PEP), was developed for use during the 2021 NICE review of the NICE Framework TKS statements and the PEP development of new TKS statements for its Privacy Workforce Framework. This guide recognizes that the "consistent use of a workforce framework's TKS statement as building blocks enables communication at a peer level, sector level, state level, national level, or international level. This communication can drive innovative solutions to common challenges, lower barriers to entry for new organizations and individuals, and facilitate workforce mobility." It identifies "general principles that apply to each of the TKS building blocks, followed by specific guidelines for drafting each individual type of statement."

The NICE Program first used the Guide when reviewing and refactoring deprecated Ability statements into TKS statements for retention and inclusion as NICE Framework data. Subsequently, the program office has used the Guide in its review of the NICE Framework Skill and Knowledge statements. What is offered here are draft updated Skill statements that follow the principles set forth in the Guide and are otherwise described below; NICE is not adding new content that would change the nature of a Work Role or address gaps at this time.

The NICE Program Office is continuing to refine and clarify the TKS statements to address unnecessary overlaps, unclear descriptions, and inconsistent phrasings, thereby helping those building blocks to be more measurable, meaningful, and useful. Additionally, this process will be an iterative one, and the NICE Program Office will conduct a full review of the updated Knowledge, Skill, and Ability statements (previously released for comment) as a whole following comment adjudication. As part of this work, we understand that there may need to be additional outreach to practitioners, particularly around new Task statements that have been developed as result of these efforts and to ensure that adjusted statements, especially ones that have been identified as redundant or duplicative, are addressed appropriately in Work Roles before integration into the NICE Framework. Finally, future work focusing on editorial adjustments to Task statements using the TKS Authoring Guide as a reference resource and will be available for public review and comment.

We understand that this review stops short of addressing gaps that are found in this process, and we expect that there will be a need to develop new statements or indeed further adjust existing statements in the future. A public commenting tool is being developed in order to allow for broad community engagement in that process, in addition to continued community engagement methods such as workshops, meetings, focus groups, and comment periods.

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 work to improve clarity and usability of the workforce framework statements. We welcome your feedback and look forward to continuing improvement of this resource.

Summary of Updates

SKILL STATEMENTS: Adjustments and Examples

Adjustments have been made to ensure that the general TKS principles, as defined in the TKS Authoring Guide, are being met. These general principles establish that TKS statements should be:

- Flexible: The statements can be applied or combined in various ways to address different local circumstances and needs. A key way Skill statements have been adjusted to meet this principle is by removing skill objectives. That is, statements only address the needed skill and do not include the reason why the skill is being employed.
  - Example: "Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures" *becomes* "Skill in interpreting debugger results"
- Consistent: The statements are drafted following common guidelines outlined in the sections below to ensure that they align with other statements and can be used in a uniform manner.
  - Examples:
    - "Skill in performing sensitivity analysis" (*original statement retained as is)*
    - "Skill in performing fusion analysis" (the original "Skill in fusion analysis" has been adjusted to align with the above for consistency)
- Clear: The statements are easy to read and understand, and not overly complex or lacking clarity.
  - Examples:
    - "Skill in identifying language issues that may have an impact on organization objectives" (*suggested withdrawal – this statement lacks clarity and is not specific to cybersecurity*)
    - "Skill in defining and characterizing all pertinent aspects of the operational environment" *becomes* "Skill in defining an operational environment" (*the language "all pertinent aspects" is ambiguous and may vary across organizations and for different projects, introducing confusion*)
- Affirmative: The statements are structured in an affirmative (i.e., grammatically positive) form to assist with the design and evaluation of performance metrics and goals and to minimize issues with language translation for organizations that work with multi-lingual teams. This is in contrast to grammatically negative statements that use language such as "do not" or "avoid."
  - Example: "Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data" *becomes the following multiple statements*:
    - "Skill in collecting digital evidence"
    - "Skill in processing digital evidence"
    - "Skill in transporting digital evidence"
    - "Skill in storing digital evidence"
- Discrete: The statements should not include more than one (compound) idea.
  - Example: "Skill in identifying and extracting data of forensic interest in diverse media" *becomes* "Skill in identifying forensic data in diverse media" *and* "Skill in extracting forensic data in diverse media"

In addition to those general principles, the review also worked to ensure that all statements meet the principles set forth specifically for Skill statements:

- Begin with "Skill in" followed by a verb. The verb is in gerund form.
    - Examples:
        - "Skill to apply analytical standards to evaluate intelligence products" *becomes* "Skill in applying analytical standards to evaluate intelligence products"
        - "Skill in information prioritization as it relates to operations" becomes "Skill in prioritizing information" (note that the "operations" context here has been removed to allow for maximum flexibility of this statement; this context may be introduced by the Work Role, Competency, or Task statement with which the Skill statement is associated)
- Represent observable actions.
    - Examples:
        - "Skill in recognizing relevance of information" (non-observable and overly broad—suggested withdrawal)
        - "Skill in using incident handling methodologies" *becomes* "Skill in handling incidents"

Finally, recommended adjustments have been made that address:

- Redundancies or duplicates. Where two or more statements are redundant with each other or duplicate content, proposed updates have been made.
    - Example: The following redundant statements, "Skill in deep analysis of captured malicious code (e.g., malware forensics)" *and* "Skill in analyzing malware" *become* "Skill in performing malware analysis" (*this update also introduces language consistent with other analysis statements, as noted above*)
- Verb consistency and clarity. During this review an analysis of Skill statement verbs was conducted. Statements that included "use" or "utilize" (including gerund forms) were either updated to introduce more active verbs or were translated into Knowledge statements. At other times, verbs have been changed to introduce consistency with like statements or to introduce clarity.
    - Examples:
        - "Skill in using outlier identification and removal techniques" *becomes* "Skill in detecting anomalies" *and* "Skill in removing outliers"
        - "Skill in using of design methods" *becomes* "Knowledge of design methods"
        - "Skill in using code analysis tools" *becomes* "Knowledge of code analysis tools and techniques"
- Parentheticals. The review identified many statements where parentheticals were included. It was decided to remove these from the statements to increase flexibility and clarity. Id est ("i.e.") parentheticals ("id est" is translated as "in other words" – therefore these statements use two ways of saying the same thing) were removed because of the redundancy and imprecision that these introduce. Exempli gratia ("e.g.") statements ("exempli gratia" can be translated as "for the sake of an example" – essentially, to mean "for instance") offer examples to illustrate the statement; although these may be informative or helpful in some circumstances, they also introduce potential issues as the examples may become outdated, may be incomplete, or may not apply to individual organizational contexts. Please note that although these have been removed in this revision, the NICE Program Office aims to reintroduce that content outside of the statements themselves in

statement “usage notes” that will be available when the NICE Framework data shifts from PDF and spreadsheet format to an online platform in 2022.

- Examples:
  - “Skill in designing a data analysis structure (i.e., the types of data a test must generate and how to analyze that data)” *becomes* “Skill in designing data analysis structures”
  - “Skill in Regression Analysis (e.g., Hierarchical Stepwise, Generalized Linear Model, Ordinary Least Squares, Tree-Based Methods, Logistic)” *becomes* “Skill in performing regression analysis”

KNOWLEDGE STATEMENTS: Adjustments and Examples

Adjustments have been made to the Knowledge statements to ensure that the general TKS principles, as defined in the TKS Authoring Guide, are being met. These general principles establish that statements should be:

- Flexible: The statements can be applied or combined in various ways to address different local circumstances and needs. Knowledge statements have been adjusted to meet this principle by removing any specificity regarding why someone would need to have the stated knowledge. Specifics of application may be provided in the Task statement versus in associated Knowledge or Skill statements.
    - Examples:
        - "Knowledge of implementing enterprise key escrow systems to support data-at-rest encryption" *becomes*
            - "Knowledge of data-at-rest encryption (DARE) standards and best practices"
            - "Knowledge of cryptographic key storage systems and software"
            - "Skill in implementing enterprise key escrow systems"
        - "Knowledge of the critical information requirements and how they're used in planning" *becomes* "Knowledge of critical information requirements"
- Consistent: The statements are drafted following common guidelines outlined in the sections below to ensure that they align with other statements in the building block category and can be used in a uniform manner. With Knowledge statements, in order to provide consistency a set of defined supporting phrases was implemented. Although not every Knowledge statement will need such a phrase, the addition of these brings to the statements consistency and clarity (see next bullet). These phrases are provided separately below.
    - Examples:
        - Principles and practices:
            - "Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation)" *becomes* "Knowledge of Confidentiality, Integrity and Availability (CIA) principles and practices"
            - "Knowledge of resource management principles and practices" *becomes* "Knowledge of resource management principles and techniques"
        - Tools and techniques:
            - "Knowledge of intrusion detection tools and techniques" *becomes* "Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions"
            - "Knowledge of cyber defense and vulnerability assessment tools and their capabilities" *becomes* "Knowledge of cyber defense tools and techniques" *and* "Knowledge of vulnerability assessment tools and techniques"
    - Supporting phrases: These phrases were derived directly from the original 2017 Knowledge statements. An in-depth review of the original statements was made to determine what language was most frequently used; this language was then refined into standard phrases for consistency. See the Knowledge statements spreadsheet for

examples of each of the below. When available, definitions are taken from the NIST Computer Security Resource Center (CSRC) Glossary.

- Authentication and authorization
    - Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
    - Authorization: The right or a permission that is granted to a system entity to access a system resource.
- Capabilities and applications
    - Capability: A set of mutually reinforcing security controls implemented by technical, physical, and procedural means. Such controls are typically selected to achieve a common information security-related purpose.
    - Application: The system, functional area, or problem to which information technology is applied. The application includes related manual procedures as well as automated procedures.
- Characteristics
    - Characteristic: A feature or quality belonging typically to a person, place, or thing and serving to identify it.
- Laws and regulations: Federal government-wide and organization-specific laws, regulations, policies, guidelines, standards, and procedures mandating requirements for the management and protection of information technology resources.
- Models and frameworks
    - Model: A detailed description or scaled representation of one component of a larger system that can be created, operated, and analyzed to predict actual operational characteristics of the final produced component.
    - Framework: A structured description of a topic of interest, including a detailed statement of the problem(s) to be solved and the goal(s) to be achieved.
- Policies and procedures
    - Policy: Statements, rules or assertions that specify the correct or expected behavior of an entity.
    - Procedure: An established or official way of doing something.
- Principles and practices
    - Principle: A fundamental source or basis of something.
    - Practice: The actual application or use of an idea, belief, or method, as opposed to theories relating to it.
- Processes
    - Process: Set of interrelated or interacting activities which transforms inputs into outputs.
- Protocols
    - Protocol: A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems.
- Roles and responsibilities
    - Role: A job function or employment position to which people or other system entities may be assigned in a system.

            - Responsibility: Something one is required to do as part of a job, role, or legal obligation.
        - Standards and best practices
            - Standard: A document, established by consensus and approved by a recognized body, that provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.
            - Best Practice: A procedure that has been shown by research and experience to produce optimal results and that is established or proposed as a standard suitable for widespread adoption.
        - Systems and software
            - System: An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.
            - Software: Computer programs and associated data that may be dynamically written or modified during execution.
        - Tools and techniques
            - Tool: A piece of software that carries out a particular function, typically creating or modifying another program.
            - Technique: A set or class of technologies and processes intended to achieve one or more objectives by providing capabilities to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems.
- Clear: The statements are easy to read and understand, and not overly complex or lacking clarity. In this review this included addressing statements that were overly complex, overly broad, vague, or otherwise difficult to comprehend.
    - Examples:
        - "Knowledge of operations security (OPSEC) principles and practices" (vs. the original "Knowledge of operations security," which is unclear due to its lack of specificity)
        - "Knowledge of planning activity initiation" becomes "Skill in initiating planning activities" (the original statement is vague, while transforming this to a Skill statement ensures its meaning and applicability is clear)
        - "Knowledge of the organization, roles and responsibilities of higher, lower and adjacent sub-elements" (*because of the lack of clarity in this statement, it is suggested that it be withdrawn*)
        - "Knowledge of data carving tools and techniques" (*this statement is straightforward and unambiguous*)
- Affirmative: The statements are structured in an affirmative (i.e., grammatically positive) form to assist with the design and evaluation of performance metrics and goals and to minimize issues with language translation for organizations that work with multi-lingual teams. This is in contrast to grammatically negative statements that use language such as "do not" or "avoid." *There were no examples of this issue in the 2017 Knowledge statements; no adjustments were made based on this principle.*
- Discrete: The statements should not include more than one (compound) idea.

- Examples:
  - "Knowledge of database administration and maintenance" *becomes* "Knowledge of database administration principles and practices" *and* "Knowledge of database maintenance principles and practices"
  - "Knowledge of analytic tools and techniques for language, voice and/or graphic material" *becomes* "Knowledge of voice analysis tools and techniques" *and* "Knowledge of graphic materials analysis tools and techniques"

In addition to those general principles, the review also worked to ensure that all statements meet the principles set forth specifically for Knowledge statements in the TKS Guide:

- Begin with "Knowledge of" followed by a concept. The core concept for the statement immediately follows "Knowledge of" so the focus of the statement is obvious. Additional information, including standard phrases (as shared above) follow the concept.
  - Examples:
    - "Knowledge of the feedback cycle in collection processes" *becomes* "Knowledge of the collection process feedback cycle" (*the primary concept, the collection process, now immediately follows "Knowledge of"*)
    - "Knowledge of the process used to assess the performance and impact of operations" *becomes*
      - "Knowledge of operation assessment processes" *and*
      - "Task: Assess operation performance" *and*
      - "Task: Assess operation impact"
- Are limited to one concept in a single statement. This principle echoes the general principle of discrete statements.
  - Example:
    - "Knowledge of multi-level security systems and cross domain solutions" *becomes* "Knowledge of multi-level security (MLS) systems and software" *and* "Knowledge of cross domain solutions"

Finally, recommended adjustments have been made that address:

- Redundancies or duplicates. Where two or more statements are redundant with each other or duplicate content, proposed updates have been made.
  - Examples:
    - The following redundant statements, "Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files" *and* "Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip)" *becomes* "Knowledge of file system principles and practices" (*this update also introduces a standard supporting phrase for additional clarification*)
    - "Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization)" *is suggested for withdrawal as being redundant with* "Knowledge of software development principles and practices" *and* "Knowledge of software design tools and techniques" *and* "Knowledge of cybersecurity principles and practices" (*note that in this case all three multiple statements may be needed to provide a full context, depending on the task, or a subset of these statements may be sufficient)*

- Organization-specific statements. To ensure that Knowledge statements are broadly applicable and support concept learning outside of any one particular organization, statements that reference specific organizational content have been adjusted accordingly.
    - Examples:
        - "Knowledge of organizational training policies" *becomes* "Knowledge of training policies and procedures"
        - "Knowledge of integrating the organization's goals and objectives into the architecture" *becomes* "Task: Integrate organizational goals and objectives into security architecture"
- Language consistency and clarity. Language adjustments address consistency and clarity.
    - Examples:
        - "Knowledge of cyber threats and vulnerabilities" *becomes* "Knowledge of cybersecurity threats" *and* "Knowledge of cybersecurity vulnerabilities" (*so that it is clear that the statement is regarding cybersecurity, rather than the much broader term cyberspace*)
        - "Knowledge of collection management processes, capabilities, and limitations" *becomes* "Knowledge of intelligence collection management principles and practices" (*here the word "intelligence" is added to clarify what type of collection management; a standard supporting phrase is also added for consistency*)
- Parentheticals. The review identified many statements where parentheticals were included. It was decided to remove these from the statements to increase flexibility and clarity. Id est ("i.e.") parentheticals ("id est" is translated as "in other words" – therefore these statements use two ways of saying the same thing) were removed because of the redundancy and imprecision that these introduce. Exempli gratia ("e.g.") statements ("exempli gratia" can be translated as "for the sake of an example" – essentially, to mean "for instance") offer examples to illustrate the statement; although these may be informative or helpful in some circumstances, they also introduce potential issues as the examples may become outdated, may be incomplete, or may not apply to individual organizational contexts. Please note that although these have been removed in this revision, the NICE Program Office aims to reintroduce that content outside of the statements themselves in statement "usage notes" that will be available when the NICE Framework data shifts from PDF and spreadsheet format to an online platform in 2022.
    - Examples:
        - "Knowledge of learning levels (i.e., Bloom's Taxonomy of learning)" *becomes* "Knowledge of Bloom's Taxonomy learning levels"
        - "Knowledge of modes of learning (e.g., rote learning, observation)" *becomes* "Knowledge of learning modes"

Links

- Draft Refactored Knowledge and Skill Statements April 2022
- National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity (NICE Framework) (NIST SP 800-181r1)
- Task, Knowledge, and Skill (TKS) Statements Authoring Guide for Workforce Frameworks (TKS Authoring Guide)
- NICE Framework Data Reference Spreadsheet (2017 Data)