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

Measuring Cybersecurity Workforce Capabilities: Defining a Proficiency Scale for the NICE Framework

Table of Contents

1. Introduction

In response to the 2017 "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,"[1] the 2018 Department of Commerce and Department of Homeland Security Report to the President[2] made recommendations that were incorporated into the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (NDAA).[3] This statute[4] provided that:

"Not later than 540 days after the date of the enactment of this Act [Jan. 1, 2021], the Director of the National Institute of Standards and Technology shall, in coordination with the Secretary of Defense, the Secretary of Homeland Security, and the heads of other appropriate agencies-

> "(1) in carrying out subsection (a) of such section [meaning 15 U.S.C. 7451(a), now 15 U.S.C. 7443(a)], assess the scope and sufficiency of efforts to measure an individual's capability to perform specific tasks found in the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST Special Publication 800–181) at all proficiency levels; and
>
> "(2) submit to Congress a report-
>
> > "(A) on the findings of the Director with respect to the assessment carried out under paragraph (1); and
> >
> > "(B) with recommendations for effective methods for measuring the cybersecurity proficiency of learners."

Since the language in the 2018 report to the President was developed and subsequently incorporated into the 2021 NDAA, NICE published the December 2020 revision of the *NICE Workforce Framework for Cybersecurity (NICE Framework)* (NIST Special Publication 800-181 Rev. 1).[5] One significant change in this revision was the introduction of Competency Areas as an additional way of leveraging the NICE Framework Task, Knowledge, and Skill (TKS) statement building blocks. As such, NIST has expanded the charge from the original NDAA language "to measure an individual's capability to perform specific tasks" in order to consider the application of proficiency levels across the NICE Framework, considering how they may be used in relation to Competency Areas, Work Roles, or even at the TKS statement levels.

NICE Framework Components

- Task, Knowledge, and Skill (TKS) Statements: The building blocks of the NICE Framework. They describe the work to be done and what someone needs to know or be able to do to complete that work.
- Competency Areas: Measurable clusters of related TKS statements that correlate with performance on the job and can be improved through education, training, or other learning experiences.
- Work Roles: A grouping of tasks for which a person or team is responsible.

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. Finally, the NICE Strategic Plan 2021-2025 includes five goals, each with multiple objectives.[6] One of these specifically calls out proficiencies:

> **Goal 3, Modernize the Talent Management Process to Address Cybersecurity Skills Gaps**
> Objective 3.3: Align qualification requirements according to proficiency levels to reflect the competencies and capabilities required to perform tasks in the NICE Framework

The recommendations that are shared in this report will be used to further this objective.

2. What is a Proficiency Scale?

This report focuses on understanding proficiency scales and how they can be used with the NICE Framework to measure a cybersecurity workforce capability. A proficiency scale provides a defined set of levels that describe the degree to which a learner possesses capability in a determined competency area.[7] Proficiency scales are used in concert with assessments to determine an individual's specific level of capability and can be used across multiple competencies. A scale serves as an agreed-upon rubric that provides a consistent means against which the capability level can be assessed. It also may be used as a measure of progress toward a capability goal.

Defining "Learner"
Throughout the NICE Framework, those performing cybersecurity work—including students, job seekers, and employees—are referenced as *Learners*. This usage highlights that each member of the workforce is also a lifelong learner.

The levels in a proficiency scale are named and broadly describe the typical behaviors associated with each proficiency level. Each level may include additional details to provide guidance for learners and assessors to better understand how a proficiency level in the defined area is determined. In this way, it can also be used to facilitate connections between the competency areas and education or training curricula.

The term "proficiency" as a standalone word is a reference to a defined level in a proficiency scale. However, the word is sometimes used informally as a shortcut placeholder for the item (e.g., task or competency) for which the proficiency is being measured. To avoid the confusion that can easily result, in this report, the term "proficiency" on its own is defined here as "level of capability as defined by a proficiency scale."

Proficiency Scale: A scale that defines specific levels of proficiency. The scale typically identifies to what the levels pertain (e.g., for specific tasks, in a course, or in a competency area) and may further define ways a level may be measured through assessment, demonstration, or other means. By providing information about what a learner requires for each level, a proficiency scale can be used to identify needed capabilities.
Proficiency: Level of capability as defined by a proficiency scale.

Proficiency Scales in the Workplace

Proficiency scales may be applied in different ways. For instance, a scale may be used to measure capability at a very narrow level (e.g., for a task) or more broadly across a competency area. Proficiency scales are used in many settings, including K-12 education, higher education, training, and within the workplace. Establishing defined proficiency levels that are designed for the cybersecurity workforce and used in a workplace environment supports the goal of ensuring the NICE Framework can be used to identify, recruit, develop, and retain cybersecurity talent for a workforce that is effective and prepared to mitigate security risks. When identifying or defining a proficiency scale specific to the NICE Framework, that application should be established within the workplace context and employed to support the needs of employers. Some key characteristics of a proficiency scale for the workplace include:

- **Demonstrative:** The workplace is where knowledge and skills come together, and demonstrating capability requires practical application versus theoretical or knowledge comprehension.[8] The scale levels should reflect how these might be evidenced in the workplace—something the NICE Framework statements can help support.
- **Supervision:** Sometimes called autonomy, direction, or oversight, many of the models that were consulted include in their level descriptions information regarding the amount and type of supervision a person might have for that level. Examples are, "substantial guidance," "little to no guidance," or "advises others." Understanding how an employee might be expected by their supervisor to perform the work at various levels of proficiency provides great insight into their capability.
- **Professional Skills:** Whether they are called professional skills, soft skills, employability skills, or any of the other numerous terms that are available, these types of skills are essential in the workplace. Different stages of a career and different work roles typically require varying levels of these skills. For instance, a leadership position may place greater emphasis on relationship building, whereas a more technical role may require greater teamwork skills. Both will need good communication skills, but likely applied in different ways. Although these are not cybersecurity-specific skills, they are nonetheless key to ensuring effectiveness in performing cybersecurity roles in the workplace.

Proficiency levels may be further combined with additional complementary measures to provide a more robust understanding of a specific position's requirements, particularly for use in personnel decisions (e.g., hiring or promotion). For instance, by including the *importance* (significance of the competency to be successful in the performance of the job) and the level of capability *required at entry* (required on day one of the job), the criticality of that competency for a position can be derived.

Proficiency vs. Career Levels

There is a distinction between levels of proficiency and career levels. Whereas a proficiency level could be a numerical range (e.g., from 1 to 5), or use descriptive language to indicate advancement across the

scale (e.g., basic, intermediate, advanced), these indicators should not be equated with a career level (e.g., early-, mid-, senior-, or executive-level[9]). There are two reasons to avoid doing this: tying these together implies that 1) career paths all have the common ultimate goal of reaching the most senior role in their field or in their organization, and 2) the higher one is in their career level, the more capable they are and that they possess greater knowledge and skills. Capability does not necessarily equate with duration in the field or in a specific role, particularly for cybersecurity, which is constantly changing and adapting to new technologies. Moreover, capability in a certain competency area may be developed outside of historically recognized (typically degree-based) learning experiences. These additional, nontraditional pathways into the field can bring experience and expertise that are not necessarily tied to longevity or seniority.

Examples of the reason to avoid specifically associating proficiency with career levels abound. Someone new to cybersecurity may arrive in an entry-level position with more current knowledge and skills in a competency area than someone who has been in the field for a decade. The wide variety of cybersecurity-related work roles means that one's proficiency level in a certain domain may not always equate to their career level. Leadership traits and capabilities can be quite different from what one needs to know when in a more technical role, and a leader may not be expected to have a high level of technological expertise, or vice versa. Further, a particular job may not require expert-level proficiency. In any event, it may not always be appropriate to require or strive for the utmost proficiency level for all jobs.

For these reasons, the models NICE has focused on define proficiency levels based on capability versus career position, which will further enable greater flexibility in applying the levels.

3. Examples of Proficiency Scales

There are many different types of proficiency scales, primarily distinguished from each other by the context in which they are meant to be used. In reviewing proficiency scales that might serve as models for a NICE Framework-applied scale, the following primary types were identified.

Educational Proficiency Scale Models

Bloom's Taxonomy

Before looking at specific educational proficiency modes, it should be noted that in academia in particular, Bloom's Taxonomy—a theoretical framework initially released in 1956 to help educators categorize learning goals—is often referenced as a tool for assessment.[10] Since proficiency levels and assessment go hand in hand, some attention to this framework is useful. At times the two are even equated—with some practitioners referencing the Bloom cognitive levels (which include remember, understand, apply, analyze, evaluate, and create) in terms of proficiency. This conflation is easily

understandable given the model's approach, presented as a hierarchical pyramid where each subsequent category builds on the preceding level(s).[11,12]

Though distinct, a proficiency scale that applies to the NICE Framework may be complementary to this model so that those who are eager to use Bloom's Taxonomy to develop learning outcomes can continue to do so. For instance, a proficiency scale that applies to the NICE Framework could be used to describe how well a learner has mastered related NICE Framework content as incorporated in outcomes developed using Bloom's model.

K-12 Educational Contexts

When applied in a K-12 education contexts, a proficiency scale is often used to measure knowledge learned more than skills applied, and assessment may be more theoretical than practical in nature. Grades in a course are a well-known example of an educational proficiency scale and are typically used to track a student's progress towards the course's learning goals. In this setting, proficiency scales usually measure at multiple levels, from individual assignments to tests and then more comprehensively at the course level (for instance, a student may receive a C grade on an assignment and an A grade on a test, averaging to a B for the course). Robert J. Marzano, author of *Proficiency Scales for New Science Standards*, describes the academic proficiency scale as having the following levels: "(1) the target (level 3.0) content; (2) the simpler (level 2.0) content; and (3) the more complex (level 4.0) content."[13]

Higher Education Contexts

In higher education there is often a shift in how levels are defined, typically taking on language that is more reflective of a workforce context. For instance, a scale may begin to introduce supervision in level determination. In one model, the amount of supervision is described at the lowest level as needing "some guidance on job duties" and then evolves into "minimal guidance," "without assistance," and then ultimately no reference to supervision or guidance at the top-most level.[14] Assessment may also start to take on a more practical application approach as well to more closely mimic the work environment.

A recent project in the Centers for Academic Excellence in Cybersecurity (CAE-C) Community on "Evidencing Competency Oversight"[15] has "devised a model for effectively and efficiently evidencing competency" that defines how to write a "competency statement" based on five traits (see Table 1):

Table 1: CAE-C Evidencing Competency Oversight Project: ABCDE Competency Statement Model

Audience or Actor	Describe the person who will be learning or performing the competency—their level of knowledge, the course or activity in which they are participating, or other information of interest.
Behavior (Performance of Task)	State the task to be done. The task should be a complete piece of work in the context of a Work Role from the NICE Framework or other framework as appropriate.
Context	Describe the scenario within which the task is to be conducted. What technology is the person provided? What documents? What limitations?
Degree	What percentage of the task is completed? What percentage correct? How long does it take?
Employability	Was the task completed in accordance with industry "best practices"? Is this "behavior" something that an employer would find satisfactory? Does this behavior require broader professional (or softer) skills?

Essentially, the CAE-C model could be looked at as a way to define the factors that go into a proficiency description about the competency being described. In this case, "behavior" defines the task to be done (derived from the NICE Framework), and the "context" field may include information akin to level of supervision, among other things. Complexity of the work to be done might also be found in "context." The "degree" and "employability" fields together describe how well the work was completed. This model provides a way of looking at how to determine someone's capability at a task level, though it stops short of defining specific proficiency levels. With a separately defined scale, this could be used as a model for assessment by various stakeholders in different scenarios (e.g., in instruction or in hiring).

Training and Certifications Contexts

The use of proficiency in training or certification programs may align even more closely with the workplace perspective. A proficiency level in this context is more likely to be described as "what a proficient employee produces and how the employee must work to achieve those results" and is akin to a "picture or snapshot of what success looks like on the job."[16] In these contexts, the means of assessment often represents how the knowledge and skills included in the program's curriculum would be applied in the workplace. That said, defined proficiency scales from training and certification providers are uncommon, or not publicly available. For example, (ISC)[2] references proficiency on their site in relation to exam scoring, and states that "proficiency is defined as meeting or exceeding the 'passing standard.'" It also gives the following for further clarification:[17]

- Below proficiency: Below the passing standard
- Near proficiency: Close to the passing standard
- Above proficiency: Above the passing standard

In this respect, the model is similar to many of the models found in the K-12 education contexts where proficiency is simply equated with meeting the target level for a course.

Another example is the MITRE Systems Engineering Competency Model that describes three levels or proficiency: Foundational, Intermediate, and Expert.[18] In this model, these proficiencies are described as cumulative: someone at a higher level would be "capable of performing the work of the levels below them." But note that the language is based in the workplace context and the descriptions of each level are task-based, indicating how knowledge and skills might be applied in the context of the workplace.

Federal Government Proficiency Scale Models

Several proficiency scale models are used in the Federal Government.[19] During a workshop held by NICE in 2021 on "NICE Framework Competencies: Moving from Concept to Implementation," [20] A Department of Homeland Security representative provided context as to how proficiencies can be used in setting targets and measuring capabilities for competencies. According to the representative, proficiency targets are foundational to the talent management lifecycle. At the early stages of the lifecycle, proficiencies play a role when drafting position descriptions, developing hiring assessments, and creating behavioral-based interview questions. Proficiencies continue to be applied after hire, in performance management and recognition and talent development, retention, and succession planning. The representative described a proficiency scale with five levels, starting with Level 0:

- Level 0: No Foundational Knowledge
- Level 1: Basic
- Level 2: Intermediate
- Level 3: Advanced
- Level 4: Expert

The model presented includes behavioral indicators that describe what is expected at each level, along with a criticality measure (see Figure 1).

Competency Definition	**Competency Definition:** This definition is like a mission statement for the Competency. It is a broad statement that sets the scope for the for the Competency.
Example Tasks Identified as Part of Competency: These tasks are included to give context around the competency. This is not meant to be an exhaustive list, but rather a few examples that came up during the conversation with the subject matter experts.	
Behavioral Indicators *(Describes how the competency manifests itself in observable on-the-job behavior)*	
0 No Foundational Knowledge	• I do not have the sufficient knowledge or skills necessary in this area for use in simple or routine work situations. Any awareness, knowledge, or understanding I do have would be considered common, similar to that of a layperson. Considered "no proficiency" for purposes of accomplishing work.
1 Basic	• I have the basic knowledge and skills necessary in this area for use and application in simple work situations with specific instructions and/or guidance.
2 Intermediate	• I have the intermediate knowledge and skills necessary in this area for independent use and application in straightforward, routine work situations with limited need for direction.
3 Advanced	• I have the advanced knowledge and skills necessary in this area for independent use and application in complex or novel work situations.
4 Expert	• I have the expert knowledge and skills necessary in this area for independent use and application in highly complex, difficult, or ambiguous work situations, or I am an acknowledged authority, advisor, or key resource in this area

Criticality		
Importance	**Required at Entry**	**Criticality**
Establishes the significance of the competency to successful performance in the occupation 1 = Not at all Important 5 = Extremely Important	Identifies the competencies required on day 1 of the job versus those that can be learned over time 1 = Not Required 3 = Definitely Required	An evaluation of Importance and Required at Entry ratings to determine which competencies could be used to make personnel decisions

Proficiency Targets			
Early Career (GS-9/11) Cybersecurity Analyst (Service Desk Analyst)	Tier 1 (GS-12/13) Associate Cybersecurity Analyst	Tier 2 (GS-13/14) Senior Cybersecurity Analyst	Tier 3 (GS-13/14/15) Cyber Threat Analyst (Technical Lead, Expert, Advisor)
Identifies the proficiency at which a person in a specific career level should be performing. *Aligns with the Behavioral Indicator descriptions above (Career levels will differ by occupation)*			

Figure 1: Measuring Proficiency of Competencies (DHS)

The U.S. Office of Personnel Management (OPM) publication, *Proficiency Levels for Leadership Competencies*, identifies a very similar five-level scale of proficiency, from level 1, awareness, to level 5, expert.[21] In this model the level of supervision required also comes into play (see Table 2). As is the case with many proficiency scales, however, the exact means of assessing the learner's attained level is not clearly defined. In this case, OPM offers the following explanation: "agencies may require applicants to provide written responses to address the competencies; answer a set of on-line questions in the application process; undergo a structured interview; or use any other appropriate assessment."[22]

Table 2: OPM Proficiency Levels for Leadership Competencies

OPM Proficiency Level	**Required Supervision**
Level 1: Awareness	Requires close and extensive guidance
Level 2: Basic	Requires frequent guidance
Level 3: Intermediate	Requires occasional guidance
Level 4: Advanced	Generally requires little or no guidance
Level 5: Expert	Serves as a key resource and advises others

The National Institutes of Health (NIH) offers a "Competencies Proficiency Scale" as "an instrument used to measure one's ability to demonstrate a competency on the job."[23] The scale identifies five levels, from fundamental awareness to expert. The model is noteworthy in that it identifies how each level has a different focus that shifts from learning to application and ultimately strategy (see Table 3); like other scales, it also includes information on level of supervision for levels 3-5, where there is a shift from knowledge-only to application.

Table 3: NIH Proficiency Scale Level Focus Areas

NIH Proficiency Scale Level	Area of Focus
1: Fundamental Awareness (basic knowledge)	Focus on learning
2: Novice (limited experience)	Focus on developing through on-the-job experience
3: Intermediate (practical application)	Focus is on applying and enhancing knowledge or skill
4: Advanced (applied theory)	Focus is on broad organizational/professional issues
5: Expert (recognized)	Focus is strategic

The Competencies at NIH website also includes a list of recommended "proficiency level from GS-1 through GS-15," though it notes that every "position is unique and the level of proficiency required … may vary."[24]

The Department of Defense (DoD) 8140 Policy Series: Management Tools for the Defense Cyberspace Workforce "takes a targeted, role-based approach to identify and develop cyberspace personnel using the DoD Cyber Workforce Framework (DCWF)."[25] The DCWF is informed by the NICE Framework. DOD Instruction 8140.02: *Identification, Tracking, and Reporting of Cyberspace Workforce Requirements* instructs that "DCWF work role codes should be determined based on analysis of the requirements of the position and the proficiency level required." [26] It identifies three levels of proficiency—basic, intermediate, and advanced—that describe depth of knowledge, amount of supervision, and complexity.

The U.S. Digital Service Subject Matter Expert Qualification Assessments (SME-QA) process includes examples of proficiencies in its job analysis toolkit, showing how proficiency scales are by no means standard and can be adjusted and customized depending on the scale's application.[27] They provide two examples: a four-level model (novice, competent, advanced, and expert) and a two-level model for assessment (meets and exceeds). Further, their definition of how proficiency is determined is also indicative of the context in which the scale is applied: "proficiencies gauge how skilled an applicant is with the given competency depending on years of experience, the scale of the organizations they've worked in, or the complexity of the projects they've participated in."[28] For the NICE Framework, such a definition introduces challenges. Cybersecurity knowledge and skill requirements are constantly evolving, with new technologies and risks regularly emerging. As stated earlier, because of this

environment, years of experience or time in the profession may not always equate with a higher proficiency. As a shift to competency- and skill-based hiring and promotion grows, it is important to distinguish proficiency as a measure of competency independent of years of service.

Finally, after consultations with multiple federal agencies, only one example of a proficiency model applied to the NICE Framework was identified. In 2021, the Federal Cyber Workforce Management and Coordinating Working Group—a volunteer interagency group that evolved out of a project focused on developing career pathways for NICE Framework Work Roles in 2019—launched a project to develop task-based interview questions using behavior indicators (BIs).[29] Using five NICE Framework Work Roles and a subset of 6-8 Task statements for each of the roles, a project team was tasked to identify BIs that represent successful task execution at specific proficiency levels. The proficiency scale that was presented to the team for application described three levels of capability based on knowledge, supervision, and complexity criteria (see Table 4). The behavior indicators developed would serve as a means of assessing the potential hire's proficiency level.

Table 4: Task-Based BI Proficiency Levels

Proficiency Level	Criteria
Foundational	• Knowledge: Basic knowledge and skills • Supervision: Frequent, specific instructions • Complexity: Simple, routine, structured situations
Intermediate	• Knowledge: Extensive knowledge and skills • Supervision: Periodic instructions • Complexity: Somewhat complicated routine and simple non-routine situations
Advanced	• Knowledge: Expert knowledge and skills • Supervision: Minimal high-level instructions or no guidance; serve as a resource to others • Complexity: Novel, ambiguous, complex, unstructured situations

This group is in the process of drafting a report summarizing this work that will serve as a guide for federal government human resources staff and hiring managers and a model for the development of additional BIs for further Work Roles and Tasks, with the understanding that individual agencies or departments may have unique requirements they would like reflected in their BIs. Because NICE Framework Task statements are written to be broadly applicable across organizations and sectors, these statements may not fully account for specific local circumstances—for example, if the work would be done via a team or an individual, if experience with a specific software application is required, or if successful completion of a task might require unique domain expertise. Consequently, measuring proficiency at a Task level may need to take individual contexts into account. Moreover, with over 1,000 Task statements in the NICE Framework and the expectation that Tasks will evolve, establishing and providing updated guidance for each Task is an effort that may not be easily scalable. However, as a

pilot project it may provide a useful model for hiring managers to use as they identify and hire to fulfill key job requirements based on individual tasks.

Proficiency Scales in the Private Sector

Proficiency scales have broad applicability for use in the private sector to support the development of a strong cybersecurity workforce. While it is more difficult to ascertain what scales are being currently used in individual companies, two distinct examples are shared below.

The IBM Kenexa Banking & Financial Services Job Skills & Competencies Framework[30]—one of 18 industry-specific talent frameworks the company provides—is similar in structure to the NICE Framework. Whereas the IBM framework sorts jobs into 11 job family groupings, the NICE Framework organizes work roles into seven overarching categories. The IBM Kenexa framework then establishes 259 competencies (which they also describe as "skills"), each with four levels of proficiency defined by 21 unique behavioral descriptions:

- Level 1: Basic understanding
- Level 2: Working experience
- Level 3: Extensive experience
- Level 4: Subject matter depth/breadth

What is different in this model from others described in this report is that the behavioral descriptions are not established by any common set of criteria (e.g., level of supervision required) and instead are very similar to what the NICE Framework would define as tasks (similar to the MITRE model above). For instance, a sample Job Profile for Retail Bank Branch Manager is provided, with a statement that this job requires extensive experience (level 3 on the proficiency scale) for the competency "Operation – Back Office"; the competency is then described with the following statements for that level:

- Works with multiple "back office" operations functions
- Evaluates major production systems and their criticalities
- Facilitates planned changes and their impact on the operations environment
- Communicates with key clients on operation-related issues
- Manages production transitions with minimal disruption
- Consults on key aspects of effective and efficient department operations

However, the lack of defined criteria means there is little consistency between proficiency levels. For example, production systems, changes, and transitions are not referenced in any of the other levels for this competency.

A second example comes from the University of British Columbia (UBC).[31] Though this is from a higher education institution, their model is a Career Framework for staff at the university that includes multiple factors: professional skills (what they call competencies),[32] core job duties, and job-related skills and

knowledge. The UBC proficiency scale defines a "level of proficiency [for each competency] based on the position within a specific Career Ladder":

1. Being Developed: the individual demonstrates a **minimal use** of the competency and is currently developing it
2. Basic: the individual demonstrates **limited use** of a competency and requires additional training to apply without assistance or frequent supervision
3. Intermediate: the individual demonstrates a **working or functional** proficiency level which enables the competency to be exercised effectively (has working or functional command of the competency)
4. Advanced: the individual demonstrates **in depth** proficiency level; is able to assist, consult or lead others in the application of a competency
5. Expert: the individual demonstrates **broad, in-depth** proficiency; is recognized as an authority or master performer in exercising the competency

There is a thread of supervision throughout these, but it is not called out consistently, and the level definitions on their own provide only limited information. UBC includes a page that describes each competency at the five levels that clarifies their intent for each competency,[33] though without defined criteria, applying this scale elsewhere (e.g., to the NICE Framework) could be challenging.

The final example, the Skills Framework for the Information Age (SFIA) framework, provides some insight into what is unique about the application of a proficiency scale in a workplace setting. The SFIA framework defines a common reference model for digital skills and competencies in a variety of domains, including cybersecurity.[34] This framework is broadly used in industry and internationally and is intended for use by those who do the work as well as those in supporting roles, such as human resources, learning and development, organization design, and procurement. The framework states "proficiency and professional competency are attained at a particular level due to the practice of that skill, at that level, in a real-world situation,"[35] and an integral part of their framework is referred to as "Levels of Responsibility":

- Level 1: Follow
- Level 2: Assist
- Level 3: Apply
- Level 4: Enable
- Level 5: Ensure, advise
- Level 6: Initiate, influence
- Level 7: Set strategy, inspire, mobilize

SFIA framework skills (which can be loosely mapped to NICE Framework Work Roles and Competency Areas[36]) are described at the levels at which they are found to be practiced within the working world. Further, because of how the levels are defined, not all SFIA skills exist at all levels. (For instance, security operations starts at level 1 but only extends to level 6, whereas governance *only* exists at levels 6 and 7).

Like the different proficiency models described above, the SFIA approach is built around specific criteria. In this case, five attributes are broadly described for each level:

- Autonomy: Akin to supervision, this factor describes the level of direction needed as well as, at the higher levels, what type of direction they provide.
- Influence: This factor describes how much interaction someone might have with others in the organization and outside of it and the level of input on decisions and strategy.
- Complexity: Describes the complexity of the work, including problem solving and strategy requirements.
- Business skills: Describes how someone communicates; works with tools, applications, and processes; approaches work; has digital skills; engages with learning and professional development; and works with security, privacy, and ethics in the workplace.
- Knowledge: Describes the extent of knowledge needed at a proficiency level, including generic, specialist, and domain knowledge.

In addition, the SFIA framework has integrated "behavioral factors"—essentially, professional skills—within the seven Levels of Responsibility across the five attributes.[37] These are described using statements of what each of these factors looks like across the levels of responsibility.

The SFIA model offers a new way of looking at how workforce proficiency is defined. Adoption of a proficiency model that aligns with or indeed replicates the SFIA approach offers multiple benefits for the NICE Framework:

- **Workforce Perspective:** It squarely focuses on proficiency in the workplace.
- **Layered Approach:** It offers a more nuanced sense of proficiency, allowing for a layered approach that accommodates simplified levels (e.g., beginning, intermediate, and advanced) in addition to the levels of responsibility.
- **Professional Skills:** It incorporates professional ("soft") skills, so that the NICE Framework could identify how those are applied to various Work Roles in a way that is useful, clear, and pertinent.
- **Career Pathways Application:** Not all roles will be appropriate for all levels of responsibility. For example, someone might need to shift from one role to another to advance in a career. For someone just entering cybersecurity, it can highlight what roles might work for them—either at the earliest of levels or when making a lateral shift from another field with the same level of responsibility. A levels of responsibility approach provides a way to consider how to navigate one's career.

Finally, the SFIA model provides an approach that could be applied in the NICE Framework to both Work Roles and Competency Areas so that the levels can be used by multiple stakeholders in multiple ways. It also helps to establish a broader context, distinct from only the ability to complete a Task—although assessments can and frequently do exist at the Task level.[38] It fills a need that is not already being well met—the need to determine an individual's overall capability to perform well in a job. By first describing what work at a particular level of proficiency looks like for NICE Framework Work Roles and Competency

Areas, it will be possible for employers, learners, and education, training, and certification providers to leverage the common language of the NICE Framework and more easily translate that into true application in the workplace.

4. Scope and Sufficiency of Current Efforts

At this time, although there is a great deal of informal discussion around proficiency levels and the need to better assess an individual's capability in cybersecurity work as defined by the NICE Framework, current efforts are insufficient. Across the federal government workforce, departments and agencies use the NICE Framework to identify staff who perform cybersecurity work, as part of the Federal Cybersecurity Workforce Assessment Act (2015).[39] Efforts to identify NICE Framework Work Roles in federal job descriptions are underway; if successful, this work could potentially be broadened to also incorporate NICE Framework Competency Areas.[40] However, efforts to identify the existing cybersecurity workforce or craft better job descriptions stop short of elucidating what proficiency in those areas means, and without a consistent and clearly defined proficiency scale in place there is a potential for discrepancy that would only serve to defeat the purpose of having a standardized scale in the first place.

Earlier work is helping to shift efforts towards a defined proficiency scale for the NICE Framework to gauge an individual's cybersecurity capabilities. As was mentioned above, in December 2020 NICE released its first revision of the NICE Framework. This revision streamlined the content of the Framework and introduced Competency Areas as another means of applying the building block Task, Knowledge, and Skill (TKS) statements. By introducing Competency Areas, it becomes possible to advance the conversation around proficiency. That includes the 2021 workshop referenced earlier, which brought together community stakeholders to explore how NICE Framework Competency Areas could be implemented, including addressing the question of proficiencies as a part of those conversations. The workshop report summarizes conversations about what would be needed in a proficiency scale and how assessments might be used.[41] As a whole, workshop participants agreed on the need for a recommended approach to proficiency or adaptable assessment model that could be revisited, evolve, and be tailored for local circumstances; they stopped short of being able to define or identify such a model.

Even prior to this, however, the question of measuring capability has been an area of focus for NICE. In 2017, the draft publication *NICE Framework Work Role Capability Indicators: Indicators for Performing Work Roles* was an early attempt to identify indicators that would signal an individual's capability and presents findings "pertaining to 99 capability indicators across Work Roles and proficiency levels."[42] This report used three levels of proficiency (see Table 5), focusing in their descriptions on attributes of knowledge, supervision, and complexity.

Table 5: Capability Indicators Proficiency Levels

Level	Description
Entry	An individual must have familiarity with basic concepts and processes and the ability to apply these with frequent, specific guidance. An individual must be able to perform successfully in routine, structured situations.
Intermediate	An individual must have extensive knowledge of basic concepts and processes and experience applying these with only periodic high-level guidance. An individual must be able to perform successfully in non-routine and sometimes complicated situations.
Advanced	An individual must have an in-depth understanding of advanced concepts and processes and experience applying these with little to no guidance. An individual must be able to serve as a resource and provide guidance to others. An individual must also be able to perform successfully in complex, unstructured situations.

This early work focuses on credentials (diplomas, degrees, and certifications resulting from education and training) and the learning (experiential and continuous) that is captured by years of experience and number of hours participating in defined learning opportunities (e.g., conferences, associations, mentoring programs).

Beyond that example, the work by the Federal Cyber Workforce Management and Coordinating Working Group to define behavioral indicators by proficiency level for specific tasks within NICE Framework Work Roles (described above) has advanced the application of proficiency to the NICE Framework and the assessment of individuals in relation to those levels. However, as noted earlier, there are questions of scalability and the effort still does not address capability at the broader Work Role or Competency Area levels. Although this approach might be useful for an employer who has a very clear set of tasks defined for a position, it stops short of being able to provide insight into how an individual might be assessed for overall capability in an area of work.

5. Recommendations

Given the insufficiency of current efforts, the following actions, to be led by the NICE Program Office in coordination with the NICE community, are recommended:

1. Establish a workplace-focused NICE Framework proficiency scale that is modeled after the SFIA Levels of Responsibility and incorporates criteria of supervision, complexity, professional skills, knowledge, and influence, to be applied to Competency Areas and Work Roles; and develop a plan to communicate the scale and its application to the NICE Framework to the community of stakeholders.
2. Encourage the NICE Modernize Talent Management Working Group to establish a Project Team for NICE Strategic Plan Goal #3: “Modernize the Talent Management Process to Address Cybersecurity Skills Gaps, Objective: Align qualification requirements according to

proficiency levels to reflect the competencies and capabilities required to perform tasks in the NICE Framework."

3. Engage stakeholders and subject matter experts to develop statements of proficiency to apply to NICE Framework Competency Areas and Work Roles that can then be used to help measure an individual's capability.

NIST believes that robust, widely understood, and participatory development processes produce the strongest, most effective, most trusted, and broadly accepted standards and guidelines. The NICE efforts will engage stakeholders throughout and consult with experts to ensure the NICE Framework is meeting community needs in order to expand its usefulness, applicability, and adoption nationwide.

Appendix: Sample Proficiency Scales

Below is a summary of the proficiency scale references in this document. These are provided in the order in which they were cited.

Competency vs Proficiency - Does It Matter?
By Brett O'Connor, Inception Training Network (LinkedIn Pulse, March 30, 2021)
https://www.linkedin.com/pulse/competency-vs-proficiency-does-matter-/

Tips From Dr. Marzano: Proficiency Scales for the New Science Standards
Marzano Resources
https://www.marzanoresources.com/resources/tips/ps_tips_archive/

What is a Proficiency Scale?
Rutland High School
https://rhs.rutlandcitypublicschools.org/academics/proficiency-based-learning-practices/proficiency-scales/

Proficiency Levels
University of Iowa, University Human Resources
https://hr.uiowa.edu/careers/competencies/proficiency-levels

CAE Initiatives: Evidencing Competency Oversight
CAE in Cybersecurity Community
https://www.caecommunity.org/initiative/evidencing-competency

Career Framework: Competency Proficiency Definitions
The University of British Columbia
https://careerframework.ubc.ca/competencies/

Competencies vs. Proficiencies
Steven Rosenbaum, C.E.O and Founder, Learning Paths International (Learning at Light Speed Weblog, March 31, 2011)
https://learningatlightspeed.wordpress.com/2011/03/31/competencies-vs-proficiencies/

(ISC)² Examination Scoring FAQs
(ISC)²
https://www.isc2.org/Register-for-Exam/Exam-Scoring-FAQs

MITRE Systems Engineering (SE) MITRE Systems Engineering (SE) Competency Model
MITRE Human Resources (September 1, 2007)
https://www.mitre.org/sites/default/files/publications/10_0678_presentation.pdf

Proficiency Levels for Leadership Competencies
U.S. Office of Personnel Management
https://www.opm.gov/policy-data-oversight/assessment-and-selection/competencies/proficiency-levels-for-leadership-competencies.pdf

Competencies Proficiency Scale
National Institutes of Health
https://hr.nih.gov/working-nih/competencies/competencies-proficiency-scale

DOD Instruction 8140.02: Identification, Tracking, and Reporting of Cyberspace Workforce Requirements
Office of the DoD Chief Information Officer (December 21, 2021)
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/814002p.PDF?ver=XEaIhBYPP_Ib2wnHOnA7xw%3D%3D

Sample Competencies & Proficiencies
U.S. Digital Service
https://smeqa.usds.gov/toolkit/job-analysis/sample-competencies-proficiencies.pdf

Behavior-Based Interview Questions Action Team Proficiency Levels
Federal Cyber Workforce Management and Coordinating Working Group
No link available.

Banking & Financial Services Job Skills & Competencies Framework: A Description of Skills and Competencies Specific to Banking and Financial Services
IBM Analytics (February 2016)
https://back.talentguard.com/wp-content/uploads/2016/08/Banking-Financial-Services-Job-Skills-and-Competency-Frameworks.pdf

Behavioural Factors Within SFIA's 7 Levels of Responsibility
SFIA Version 8
https://sfia-online.org/en/sfia-8/behavioural-factors-in-sfia

National Initiative for Cybersecurity Education (NICE) Framework Work Role Capability Indicators: Indicators for Performing Work Roles (Draft NISTIR 8193)
Stein, Daniel, et al. (November 2017)
https://csrc.nist.gov/CSRC/media/Publications/nistir/8193/draft/documents/nistir8193-draft.pdf

Endnotes

[1] Trump, Donald J. (May 11, 2017). *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Retrieved 10 May 2022 from https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[2] The Secretary of Commerce, The Secretary of Homeland Security (November 16, 2017). *A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future*. NIST. Retrieved 10 May 2022 from: https://www.nist.gov/system/files/documents/2018/07/24/eo_wf_report_to_potus.pdf

[3] *Public Law 116 - 283 - William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*. Congress.gov. Retrieved 10 May 2022 from: https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf

[4] Ibid; see Title XCIV—Science, Space, and Technology Matters, Subtitle A—Cybersecurity Matters, Sec. 9401(d): *Proficiency to Perform Cybersecurity Tasks*.

[5] Petersen, Rodney, et al (November 2020). *NIST Special Publication 800-181 Rev. 1, Workforce Framework for Cybersecurity (NICE Framework)*. NIST. Retrieved 10 May 2022 from https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final

[6] *National Initiative for Cybersecurity Education (NICE) Strategic Plan (2021-2025).* Retrieved 15 April 2022 from https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan

[7] Although there is no standardized number of levels prescribed for proficiency scales, most seem to focus on three to five levels.

[8] See, for instance, how competency is defined in the *LinkedIn Pulse* news article, "Competency vs Proficiency - does it matter?" by author Brett O'Connor from the Inception Training Network (March 30, 2021): "If Competency is if you 'could' do the job in theory, proficiency could be demonstrated when you do the job in the real world." Retrieved 15 April 2022 from https://www.linkedin.com/pulse/competency-vs-proficiency-does-matter-/

[9] The career levels given here are derived from the *Society for Human Resource Management (SHRM) Competency Model* (https://www.shrm.org/LearningAndCareer/competency-model/PublishingImages/pages/default/SHRM%20Competency%20Model_Detailed%20Report_Final_SECURED.pdf). This document mentions proficiency throughout but does not design proficiency levels. Instead, it provides a list of "Proficiency Standards by Career Level"—essentially, a list of statements that describe expected indicators for each career level (e.g., "Reports trends to leadership"). Some models attempt to align proficiency levels with career level. See, for instance, the U.*S. Department of Health and Human Services (HHS) Competency Framework*, which associates competencies according to basic leadership, supervisory, managerial, and executive career levels (https://humancapital.learning.hhs.gov/competency/framework.asp).

[10] For more information, see "Bloom's taxonomy" (18 March 2022), *Wikipedia*. Retrieved 15 April 2022 from https://en.wikipedia.org/wiki/Bloom%27s_taxonomy

[11] Armstrong, P. (2010). *Bloom's Taxonomy*. Vanderbilt University Center for Teaching. Retrieved 15 April 2022 from https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/

[12] Views differ about the model as a hierarchy, with some questioning the "existence of a sequential, hierarchical link" between the categories and "distinction between the categories can be seen as artificial since any given cognitive task may entail a number of processes." See: https://en.wikipedia.org/wiki/Bloom%27s_taxonomy#Criticism_of_the_taxonomy

[13] *Tips From Dr. Marzano: Proficiency Scales for the New Science Standards*. Marzano Resources. Retrieved 15 April 2022 from https://www.marzanoresources.com/resources/tips/ps_tips_archive/. Another example, provided by Rutland High School, uses a point scale, ranging from 0.0 ("little or no evidence of the student having met the standard") to 4.0 ("the student has gone above and beyond to demonstrate mastery of the skill"). It is interesting to note that this scale allows students to be assessed with half-points (e.g., 2.5) and particularly its assertion that "a score of 3.0 indicates proficiency within a standard. In other words, a student receiving a score of 3.0 has met the standard." So, in this model, 3.0 is the gold standard, although it does include a measure for students who exceed even that. (What is a proficiency scale? *Rutland High School*. Retrieved 15 April 2022 from https://rhs.rutlandcitypublicschools.org/academics/proficiency-based-learning-practices/proficiency-scales/)

[14] See, for example, "Proficiency Levels" from the University of Iowa, University Human Resources. This example gives four levels of proficiency, ranging from basic to working, extensive, and, finally, expert/leader. Retrieved 15 April 2022 from https://hr.uiowa.edu/careers/competencies/proficiency-levels.

[15] *CAE Initiatives: Evidencing Competency Oversight*. CAE in Cybersecurity Community. Retrieved 15 April 2022 from https://www.caecommunity.org/initiative/evidencing-competency

[16] Rosenbaum, Steven (March 31, 2011). Competencies vs. Proficiencies. *Learning at Light Speed Weblog*. Retrieved 15 April 2022 from https://learningatlightspeed.wordpress.com/2011/03/31/competencies-vs-proficiencies/

[17] *(ISC)² Examination Scoring FAQs*. (ISC)². Retrieved 15 April 2022 from https://www.isc2.org/Register-for-Exam/Exam-Scoring-FAQs

[18] MITRE Human Resources (September 1, 2007). *MITRE Systems Engineering (SE) MITRE Systems Engineering (SE) Competency Model*. MITRE. Retrieved April 15, 2022 from https://www.mitre.org/sites/default/files/publications/10_0678_presentation.pdf

[19] Note that the discussion of federal proficiency scale models here does not include the narrow use of this approach when assessing language proficiency, as it has limited applicability to how such a model might relate to other subject areas. See, for instance, the U.S. Department of State site, *What are the Language Proficiency Definitions?* (https://careers.state.gov/faq-items/language-proficiency-definitions/)—which defines a six-level scale (from 0, for no proficiency, to 5, native or bilingual proficiency). Another example of language proficiency testing is produced by the Defense Language Institute and used by the U.S. Department of Defense: the *Defense Language Proficiency Test (DLPT)* (https://www.dliflc.edu/resources/dlpt-guides/). This test uses *Interagency Language Roundtable (ILR) Proficiency Skill Level Descriptions,* which rates language proficiency from 0 to 5 (https://www.govtilr.org/Skills/ILRscale2.htm).

[20] Wetzel, Karen A. (May 5, 2021). *NICE Framework Competencies: Moving from Concept to Implementation - Workshop Report*. NIST. Retrieved April 15, 2022 from https://www.nist.gov/system/files/documents/2021/06/09/NICE%20Framework%20Competencies%20Workshop%20Report.pdf

[21] *Proficiency Levels for Leadership Competencies*. U.S. Office of Personnel Management. Retrieved 15 April 2022 from https://www.opm.gov/policy-data-oversight/assessment-and-selection/competencies/proficiency-levels-for-leadership-competencies.pdf. OPM has created the CEDAR—Competency Exploration for Development and Readiness—assessment tool as a way to put into practice the Proficiency Levels for Leadership Competencies. It "uses employee self-assessment and supervisor proficiency ratings to guide training and development needs." See https://cedar.opm.gov

[22] *Frequently Asked Questions: Qualifications*. U.S. Office of Personnel Management. Retrieved 15 April 2022 from https://www.opm.gov/faqs/QA.aspx?fid=eee2a0b7-6501-42e3-ba3a-627cff1df54f&pid=ccb270fa-6027-411b-acdf-bb3302560369

[23] *Competencies Proficiency Scale*. National Institutes of Health. Retrieved 15 April 2022 from https://hr.nih.gov/working-nih/competencies/competencies-proficiency-scale

[24] Office of Human Resources. *Competencies at NIH: Suggested Proficiency Map*. National Institutes of Health. Retrieved 15 April 2022 from https://hr.nih.gov/working-nih/competencies/occupation-specific/suggested-proficiency-map

[25] The Department of Defense Chief Information Officer, Cyber Workforce Management Directorate (Spring 2022). "Department of Defense 8140 Policy Series: Management Tools for the Defense Cyberspace Workforce" *NICE eNewsletter*. Retrieved 15 April 2022 from https://www.nist.gov/itl/applied-cybersecurity/nice/nice-enewsletter-spring-2022-government-spotlight.

[26] Office of the DoD Chief Information Officer (December 21, 2021). *DOD Instruction 8140.02: Identification, Tracking, and Reporting of Cyberspace Workforce Requirements*. Washington Headquarters Service. Retrieved 15 April 2022 from https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/814002p.PDF?ver=XEaIhBYPP_Ib2wnHOnA7xw%3D%3D

[27] U.S. Digital Service. *Sample Competencies & Proficiencies*. SME-QA Hiring Strategy. Retrieved 15 April 2022, https://smeqa.usds.gov/toolkit/job-analysis/sample-competencies-proficiencies.pdf

[28] Ibid, p.1

[29] This work was under the auspices of a Federal Cyber Workforce Management and Coordinating Working Group "Interview Action Team" launched in 2021.

[30] IBM Analytics (February 2016). *Banking & Financial Services Job Skills & Competencies Framework: A description of skills and competencies specific to Banking and Financial services*. TalentGuard. Retrieved 15 April 2022 from https://back.talentguard.com/wp-content/uploads/2016/08/Banking-Financial-Services-Job-Skills-and-Competency-Frameworks.pdf

[31] *Career Framework: Competency Proficiency Definitions*. The University of British Columbia. Retrieved 15 April 2022 from https://careerframework.ubc.ca/competencies/

[32] The University of British Columbia Career Framework identifies 16 professional skills—what they call competencies: accountability, analytical thinking, building relationships, business enterprise knowledge, business process knowledge, change advocate, collaboration, communication for results, information systems knowledge, initiative, leading others, leading the organization, leading self, problem solving, strategic technology planning, and thoroughness. See *Competencies and Definitions* retrieved 15 April 2022 from https://careerframework.ubc.ca/competencies/competencies-and-definitions/

[33] Ibid.

[34]SFIA—the Skills Framework for the Information Age—was first published in 2000. See https://sfia-online.org/en

[35] *The Context for SFIA*. SFIA. Retrieved 15 April 2022 from https://sfia-online.org/en/about-sfia/the-context-for-sfia

[36] SFIA has published detailed mappings of their framework to both NICE Framework Work Roles (*Mapping SFIA 8 skills to NICE work roles*, retrieved 15 April 2022 from https://sfia-online.org/en/tools-and-resources/sfia-views/sfia-view-information-cyber-security/mapping-nice-work-roles-to-sfia-skills) and the NIST Cybersecurity Framework (*SFIA as an informative resource for the NIST Cybersecurity framework*, retrieved 15 April 2022 from https://sfia-online.org/en/tools-and-resources/sfia-views/sfia-view-information-cyber-security/sfia-as-an-informative-resource-for-the-nist-cybersecurity-framework).

[37] Thirteen behavioral factors are described (collaboration, communication skills, creativity, decision making, delegation, execution performance, influence, leadership, learning and professional development, planning, problem solving, security, privacy and ethics, and contextual and attribute descriptions). SFIA Version 8, *Behavioural factors within SFIA's 7 levels of responsibility*. Retrieved 15 April 2022 from https://sfia-online.org/en/sfia-8/behavioural-factors-in-sfia

[38] Competitions provide a way for individuals to test their ability to perform individual tasks. See, for example, the NICE Challenge project: https://nice-challenge.com

[39] The Federal Cybersecurity Workforce Assessment Act (2015) requires agencies to identify and code positions using the NICE Framework and identify and annually report on cybersecurity work roles of critical need through 2022. See the Office of Personnel Management *Policy, Data, Oversight: Human Capital Management* webpage, which links to the Act and includes resources "available to help agencies understand and implement the requirements of the Act": https://www.opm.gov/policy-data-oversight/human-capital-management/cybersecurity/

[40] This effort is currently being pursued by leadership of the Federal Cyber Workforce Management and Coordinating Working Group. For more information, visit https://community.max.gov/display/Management/Federal+Cyber+Workforce+Management+and+Coordinating+Working+Group

[41] Wetzel, *NICE Framework Competencies*.

[42] Stein, Daniel, et al (November 2017). *National Initiative for Cybersecurity Education (NICE) Framework Work Role Capability Indicators: Indicators for Performing Work Roles (Draft NISTIR 8193)*. NIST. Retrieved on 15 April 2022 from https://csrc.nist.gov/CSRC/media/Publications/nistir/8193/draft/documents/nistir8193-draft.pdf