Please consider the attached recommendations for inclusion in the next version of the NICE Framework. Based on our experience in the cybersecurity industry, we are more than willing to work with your sub-committees to build the KSATS for the new recommended Work Roles outlined in this RFC response.

Thanks,

Thomas Trevethan, Ph.D. | Curriculum Manager
Palo Alto Networks | 3000 Tannery Way | Santa Clara, CA 95054 | USA
www.paloaltonetworks.com

Thomas Trevethan, Ph.D.

Curriculum Manager

Palo Alto Networks Cybersecurity Academy

The public is encouraged to provide input either by mailing them to NICE Framework Request for Comments, National Institute of Standards and Technology, 100 Bureau Drive, Stop 2000, Gaithersburg, MD 20899; or via email to nicframework@nist.gov. Please put "NICE Framework Request for Comments" in the subject line of the email. Deadline - 1/13/2020.

Request for Comments (RFC) – NIST.SP.800-181

The following topics are intended to help NIST and its partners who are part of the NICE Community to learn about experiences in applying and using the NICE Framework and explore opportunities for improvement.

1. Describe what components of the NICE Framework have been most useful to you and why.

   Categories, Work Roles, and KSATS. Curriculum development teams are able to systematically map the KSATS to course content as well as hands-on labs in order to effectively prepare students for the specific work roles based on pathways within their area of study.

2. Describe what components of the NICE Framework have been least useful to you and why.

   There is some overlap of KSATS between Work Roles and some of the KSATS may not be relevant to individual Work Roles.

3. Share any key concepts or topics that you believe are missing from the NICE Framework. Please explain what they are and why they merit special attention.

There are a number of relevant cybersecurity work roles that are missing from the current version of the Framework. See recommendations in section 7 below.

4. Describe how the NICE Framework can be more useful to a variety of audiences (i.e. employers, employees, education and training providers, learners, small enterprises, etc.).

   For the academic audience, there should be grade appropriate work roles or modules of work roles that lead to a final role after the KSATS within those modules collectively have been learned. This possibly can be addressed in the form of pathways or badging where a student would embark on an educational path leading to a work role through academic progression over a period of time.

5. Describe the potential benefits or challenges experienced when aligning the NICE Framework more closely with other related standards, guidance, or resources (e.g., NIST Framework for Critical Infrastructure Cybersecurity, NIST Privacy Framework, other NIST Special Publications, etc.).

   It is difficult to align the Framework to High School CTE programs since the standards significantly vary on a State by State basis. It would be great if the NICE Framework could address the lower level high school work roles separately since not all students attend college directly out of high school.

6. Explain if you think the scope of the covered workforce as stated by the NICE Framework needs to be adjusted.

   The scope definitely needs adjustment in order to keep up with the emerging work roles and technologies in this dynamic landscape of cybersecurity education.

7. Describe any improvements that might be made in the current organization of the NICE Framework and its major components such as Categories, Specialty Areas, Work Roles, Knowledge, Skills, Abilities, and Tasks.

   The Framework revision should include new and emerging work roles based on the current and future cybersecurity industry. Here is a list of work roles that should be considered:

a. Network Security Engineer

Network security engineers are responsible for the provisioning, deployment, configuration, and administration of many different pieces of network and security-related hardware and software. These include

firewalls, routers, switches, various network-monitoring tools, and virtual private networks (VPNs).

b. Cloud Security Administrator

The Cloud Security Administrator will support clients in their cloud operations to enhance, optimize, and maintain computing capabilities across their technical landscape. This includes working with Cloud Architects when interviewing clients to understand application and infrastructure current state. The position will support Cloud Architects leading client working sessions to identify, categorize, prioritize and analyze data and information to work into cloud migration action plans. Cloud Security Administrators also work with the larger project teams to migrate legacy applications to their cloud platform.

c. Cloud Security Analyst

Cloud Security analysts are responsible for ensuring that the company's digital assets are protected from unauthorized access. This includes securing both Online and On-Premise infrastructures by analyzing metrics and data to filter out suspicious activity, and mitigating risks before breaches occur. If a breach does occur, security analysts are often on the front line leading efforts to counter the attack. Security analysts are also responsible for generating reports for IT administrators and business managers to evaluate the efficacy of the security policies in place.

d. Cloud Security Engineer

A cloud security engineer specializes in providing security for cloud-based digital platforms and plays an integral role in protecting an organization's data. This may involve analyzing existing cloud structures and creating new and enhanced security models and methods. They often serve as part of a larger team dedicated to cloud-based management and security.

e. Cloud Security Architect

The Cloud Security Architect will lead the design and development of security architectures for protecting PHI/PII/PCI data deployed into different types of cloud and cloud/hybrid systems. Cloud Security Architects directly contribute to the overall global enterprise cloud architecture and lead the security vision and strategy around cloud-based applications, across all topologies (including Infrastructure, Platform, and Software as a Service (IaaS/PaaS/SaaS).

f. Security Operations Center (SOC) Analyst - Systems Security Analyst OM-ANA-001

Recommend adding these KSATS to the Systems Security Analyst Work Role OM-ANA-001 as well as introducing SOC (Security Operations Center) in the work role description.

The Security Operations Center Analyst will:

- ***Task - Identify system components, evaluate architectural options, and choose among deployment options***
- ***Skill required to Install server, engine, and configure live backups***
- ***Knowledge of how to evaluate/validate baseline system functions***
- ***Skill in performing ongoing maintenance, encompassing content updates,***
backups, updates, upgrades, licensing and miscellaneous customizations
- ***Task - Troubleshoot common problems through use of recommended Security Operating Center resources and procedures***
- ***Ability to customize and/or fine tune cybersecurity system configuration/operational parameters***
- ***Ability to maintain multi-tenant cloud deployment models***
- ***Skill required to add or install a remote database***
- ***Skill in configuring integrations***
- ***Knowledge and understanding of how to monitor system health***

g. Security Operations Center (SOC) Engineer

Through the application of industry-standard security frameworks, the SOC Engineer will define, implement, operate, and optimize processes such as Site Reliability Engineering (SRE) and technologies to secure information technology infrastructure. The role is highly cross-functional and will engage stakeholders throughout the organization, instilling a culture of security practices among IT, engineering, and business unit teams.

h. Security Operations Center (SOC) Architect

Security Operations Center (SOC) Architects will work directly with clients around Security, Information, Event Management (SIEM) systems, and DEVSECOPS including development, testing, deployment and ongoing maintenance/support.

8. Describe how the NICE Framework can best document and describe Knowledge, Skills, Ability, and Task statements as well as Competency Areas.

It would be beneficial to include a video and perhaps an interactive learning component that will introduce and summarize the framework itself and how it can be used. Here is an example of what the Australian National Workforce Development group uses to introduce the NIST/NICE Framework.

https://www.austcyber.com/resources/dashboards/NICE-workforce-framework

9. Explain whether the NICE Framework indicates which Knowledge, Skills, and Abilities could be considered as foundational for all workforces that regularly interact with networks, systems, and data in cyberspace.

   Not sure this is fully explained in the NIST.SP.800-181 but you can see that K0001 through K0006 are listed in all 52 Work Role detail listings in appendix B. There may be other KSATS that span across all roles and it could be argued that at a minimum K0001 through K0010 should be considered foundational to all work roles.

10. For each NICE Framework work role, please provide an informative reference that you would like the NICE Framework Resource Center to reference.

    It is possible that this is already referenced in documentation other than the NIST.SP.800-181 but it would be great if we could include references to the U.S. Bureau of Labor Statistics https://www.bls.gov/home.htm or CyberSeek https://www.cyberseek.org/index.html to align the NIST/NICE Work Roles with industry jobs and career projections.

11. Describe which components of the NICE Framework you think are best left as static content and would not change until the next revision and which components could be managed as dynamic content (i.e., more frequent changes or updates to accommodate new information as it becomes available).

    The top 7 categories should remain static but the work roles and related KSATs should be managed as dynamic content with more frequent updates since the cybersecurity industry changes so rapidly.

12. Describe the value or risk in different organizations, sectors of the economy, or organizations with classified versus unclassified workforces to develop customized versions of the NICE Framework tailored to their specific circumstances.

    If an organization is leveraging the NICE Framework to build a customized version of their own Framework, there is minimal risk as long as the document remains internal and shared only with employers who would potentially hire employees that match the classified work roles.

Awareness, Applications, and Uses of the NICE Framework

Recognizing the critical importance of widespread voluntary usage of the NICE Framework to achieve the goals of Executive Order 13870 on America's Cybersecurity Workforce, NIST solicits information about awareness of the NICE Framework and its application and use by organizations and by individuals.

1. Describe the extent of current awareness of the NICE Cybersecurity Workforce Framework within your organization or sector or among individuals.

   There is a high level of awareness within the content development department of our company.

2. Describe how you or your organization was introduced to the NICE Framework.

   Former college professor was hired to develop an academic program for the Cybersecurity Academy and introduced the Framework based on previous exposure in Academia.

3. Describe the greatest challenges and opportunities for increasing awareness and use of the NICE Framework.

   Special Publication NIST.SP.800-181 is a lengthy document and it would be easier to understand if the KSATS were positioned in order. Starting with table 4 on page 24 it would be great if we started to list the KSATS here in the order of Knowledge, Skills, Abilities, and Tasks instead of starting out with Tasks, Knowledge, Skills, and Abilities.

   In order to improve navigation, the Framework should include Hyperlinks in the table of contents in order to quickly move to specific sections within the document.

   Appendix B – Work Role Detail Listing should be positioned more prominently in the beginning section of the document before moving through the KSAT details in order to provide the reader with a big picture of what the individual work roles look like when combined with the categories and KSATs.

4. Explain how you are currently referencing (i.e., applying or using) the NICE Framework and what plans, if any, you have for referencing it during the next year.

   Our curriculum development team is currently mapping all academic courses to selected work roles within the framework as they relate to our technology. The development team plans to increase the use of the Framework by recommending new and emerging work roles that pertain to

the cybersecurity industry and are missing from the current version of the Framework.

5. If you are an employer, describe how your organization uses the NICE Framework to develop position descriptions, guide skill-based training, facilitate workforce planning, or other uses.

   Currently not using the Framework in this manner.

6. If you are an education or training provider, describe how your organization uses the NICE Framework to develop or describe education and training content or associated credentials.

   For Academic courses, our curriculum development team currently use a custom 7 step ADDIE model to develop curriculum as listed below:

Step 1 – Define Academic Course Name(s) and Domains (ANALYSIS)
Step 2 – Design Course Objectives based on Domain Categories (DESIGN)
Step 3 - Select Work Role from the NIST/NICE Framework NIST 800-181 (DESIGN)
Step 4 – Align/MAP Work Role KSATS to Domains (DESIGN)
Step 5 – Develop lab environment based on Work Role Skills (DEVELOP)
Step 6 – Develop Syllabus, Content, Media, Labs, and Assessments (DEVELOP)
Step 7 – Implement on Moodle (LMS) Platform (IMPLEMENT/EVALUATE)

7. If you are an employee, job seeker or learner, describe how you use the NICE Framework for communicating your competencies or skills to employers, identifying training or professional development needs, or navigating your career pathway.

   We are currently not using the Framework in this manner.

8. Describe any tools, resources, or publications that exist that reference or would benefit by referencing the NICE Framework.

   Here is an example of what the Australian National Workforce Development group uses to introduce the NIST/NICE Framework:
   https://www.austcyber.com/resources/dashboards/NICE-workforce-framework

9. Describe any tools, resources, or technical support needed to increase the application and use of the NICE Framework.

   N/A

10. Propose any improvements for the application and use of the NICE Cybersecurity Workforce Framework.

It would be beneficial to include a video and perhaps an interactive learning component that will introduce and summarize the framework itself and how it can be used.