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

   The broad categories help people (students) begin to comprehend the very different career paths that are available.

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

   No response.

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.

   As data science, machine learning, automation and Artificial Intelligence are being adopted within several areas of cybersecurity (forensic analysis, cyber defense, etc.), the Framework should include some mention of these terms in several different workroles.

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.).

   More clarity is needed in the terms Knowledge, Skills and Abilities, and an understanding of how to distinguish between them, particularly for the private sector where these terms are not as common. This is particularly needed for HR and hiring managers at employers to be able to adopt the NICE Framework into their existing hiring & talent management processes.

   Create templates / use cases that illustrate how to use the Framework as an employer, employee, education /training provider, small business, etc. Must also articulate potential benefit of using the Framework to each audience. Recommend aligning these use cases & benefits with strategies that have been articulated to close the workforce skills gap, e.g., https://securityintelligence.com/articles/3-workforce-strategies-to-improve-the-state-of-jobs-in-cybersecurity/, recommendations from Aspen Group, etc.

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.).

   No response.

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

   Use the terminology of *cyber domain* not *cybersecurity* to better align with continued evolution of our understanding of things, as evidenced by DoD. The term cybersecurity seems to make it easy for individuals to think the Framework doesn't apply to them because their job isn't "cybersecurity".

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.

   Better definition/delineation of what should be considered Knowledge, Skill or an Ability would be helpful. Also, an approximate indication for each workrole of whether novice, journeyman or expert level is appropriate for each of the 6 common KSAs would be helpful - what is reasonable to expect a software developer to know about risk management processes is likely rather different than a CISOs.

   Also K0004's "cybersecurity and privacy principles" is not defined, and I am unaware of any NIST publication that defines these principles? I believe it may be a reference to the goals of cybersecurity, eg.

the CIA triad (confidentiality, integrity, availability) augmented with authentication, authorization, privacy and anonymity, but I am not certain. This KSA needs clarification – at least provide a reference to where these principles are defined.

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

   Provide clear, concise definitions and a worked example that illustrates how related aspects can be categorized /defined. For example, does NIST/NICE agree with the definition/usage on this page: https://www.staffsquared.com/blog/the-difference-between-knowledge-skills-and-abilities/?

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.

   There are 6 KSAs that appear to be "foundational" – they are found in every work role. However, those 6 KSAs are somewhat vague, and use terms with significant ambiguity such as "risk".

   Those 6 KSAs are not one size fits all – some work roles require rudimentary knowledge or familiarity with those KSAs, other work roles expect master of some or all of those KSAs. many of the KSAs are (understandably) written without any indication of the expertise required for that KSA in that specific

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

    No response.

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).

    Categories, specialty areas and workroles are probably static, however, some Tasks & KSAs may need to be refined, particularly as data science, machine learning, automation and Artificial Intelligence are being adopted within several areas of cybersecurity (forensic analysis, cyber defense, etc.).

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.

    There is little value or risk to different entities as described for customized versions of the NICE Framework at this time. The Framework has not been sufficiently adopted and evaluated in organizations to assume that entities within a sector of the economy or orgs with both class/unclass workforce are similar enough to warrant anyone spending time to create customized versions of the current NCWF. When there is substantive feedback on the Framework after being used to actually attempt alignment in education, prospective job seekers and open positions in the private sector, then perhaps consider creating industry specific customizations.

Awareness, Applications, and Uses of the NICE Framework

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

   In the general software development industry, there appears to be very low awareness of NCWF, except for organizations that have mature DevSecOps processes or which are required to use the NIST Risk Management Framework.

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

   I was one of the SMEs involved in creating the original version.

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

   Adoption of the Framework is impeded by hiring managers, HR, and/or individual employees that believe "Job X isn't cybersecurity." Supporting roles in IT and elsewhere in the organization are still being overlooked, perhaps because the term cybersecurity is used rather than just "cyber".

   Education and Industry don't know how to apply the Framework in their individual spheres and they lack any actual incentive to do so. Each expects the other to go first. They need a) concrete use cases that illustrate potential benefit of using the Framework to educate, recruit, train and retain employees; b) guidance in mapping existing job descriptions into the Framework; and c) how to use the Framework to create training & development plans.

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.

   We integrated the NICE Framework into Comic-BEE, a cybersecurity education technology for created branching web comics aligned with instructional goals that was developed with funding from DHS. Authors can choose their own instructional goals, or select NICE Framework categories, specialty areas, work roles and specific tasks & KSAs when creating the stories for education or assessment.

   I use the NICE Framework to help middle school teachers and administrators understand there are many different types of cyber careers possible and illustrate that not every cyber job requires coding or "hacking".

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.

   The organization does not use NCWF at this time.

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.

   Not applicable.

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.

   No Response.

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

   No Response.

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

a. As mentioned above, document the Use Cases for educators & employers to align courses/degrees/positions with the Framework, with ROI and/or benefit clearly articulated.

b. Provide workshops / webinars for higher ed institutions (cybersecurity faculty, curriculum designers, program managers etc.) in how to rapidly map courses into NICE Workforce Framework; this shouldn't be something that requires significant faculty effort. Do this at 3CS, for example, or CISSE, as part of existing conferences.

c. Do active outreach to get outside the Collegiate Subgroup members by targeting & reaching more post-secondary institutions who offer cybersecurity programs or certificates or minors, as well as those with Computer Science or Human Factors or AI or related degree programs and get them to map coursework into NICE Workforce Framework.

d. Provide & promote an "individual skills portfolio" capability that allows individual practitioners to map their workroles and tasks, and self-assess their KSAs – so that they can do what is described in Question 7 above. Eventually, grow that to the next level: help individuals find micro-certifications, badges, or other assessments to verify their self-assessments by providing links to education/training provider offerings that map to those same workroles/tasks/KSAs. (The NICCS portal doesn't truly support this, it is an unfriendly UI and search capability, unless you're already an expert in all things cyber, NICE Workforce and NICCS portal).

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

    See 9 immediately above. Also, reach out to the broader cyber / infosec community: there are MANY infosec conferences every year filled with practitioners and it seems too many of them have never heard of the NICE Framework.

    Best regards,

Laurin Buchanan, CISSP
Principal Investigator
Secure Decisions, a division of Applied Visions, Inc.
www.securedecisions.com