Below are comments from CertNexus on the NICE Framework. Please contact mbranch@certnexus.com with any questions.

Improvements to the NICE Framework

1. Describe what components of the NICE Framework have been most useful to you and why. ***The work roles, their KSAT's are useful as we map our certifications to them.***

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

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. ***Emerging Technologies***

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.).

    Note on "Academic institutions" in first sentence, second para. Might want to change to "academic and training institutions" to include those organizations outside of academia that are providing education.

    Include an appendix that includes resources such as certifications, cyber ranges, apprenticeships.

    Some of the work roles have titles and descriptions that seem jargon-y or specific that may not apply outside the government, such as "All-Source Analyst" and "Target Network Analyst" or that could be clearer to those not operating in the government space. Provide broader terms, definitions, or descriptions that are applicable outside the government. OR, provide a glossary that defines these terms that make them more accessible to educators/training organizations not operating within the government sector. work roles are represented very linearly,

    Present work roles as a path to other job functions/work roles.

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 comment***

6. Explain if you think the scope of the covered workforce as stated by the NICE Framework needs to be adjusted. ***Work Roles in the Protect and Defend category: does Cyber Defense Infrastructure Support fit here? We feel it might fit better in a different category. The work roles in the PR category, most of the others are reactive (to an event) while this one is more proactive (long before an event). Even the description reads differently More suited to Securely Provision or Operate and Maintain category. Does this apply in government and large-scale corporations—do they have a very specific job function that supports the infrastructure that is specific to a cyber defense system? Smaller organizations don't have such a specific function—those job functions would just be included as part of the usual***

infrastructure support roles. Does this apply, then, to all organizations that the framework might support?

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.

   KSAs and Ts are separated. Do they have the same weighting, or do the KSAs matter more than the Tasks, or vice versa? From a student perspective, what does that mean to me? Are they evaluated differently? How do I prepare for one or the other?

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

   Background – perhaps might be helpful to have a little more detail about how the Categories, Specialty Areas, Work Roles (titles and descriptions), KSAs and Ts. For instance:

   - *How were they created and mapped? Who worked on each component?*
   - *Were Job Task Analyses conducted, or some other form of input used?*
   - *Did the same people come up with the KSAs/Ts that mapped them to work roles?*

   In general, it might be useful to provide a more detailed summary of how the components of the framework were devised beyond the short summary included. "

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 is a large preponderance of K items that apply to multiple work roles. Potentially instead a line item that subsumes those cross-functional Ks into a "prerequisite knowledge" or "fundamental knowledge" that applies to a number of job functions or work roles. "Entry level" or "baseline" level of knowledge that can be used to help someone assess whether a work role is suitable for an employee/candidate/individual looking at a job function.*

10. For each NICE Framework work role, please provide an informative reference that you would like the NICE Framework Resource Center to reference. *No comment*

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). *It is our belief that content should be as static as possible given the process to update. The exception to this would be only if it becomes a fully dynamic tool which is updated continually.*

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. ***No comment***

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. ***We are primarily aware of this through its alignment with 8570/8140 directive. We also utilize to provide mapping to job seekers/ changers who are seeking employment by or reimbursement by company or organization.***

2. Describe how you or your organization was introduced to the NICE Framework. ***As alignment to 8570 and through c3 as a standard used to validate cybersecurity work roles.***

3. Describe the greatest challenges and opportunities for increasing awareness and use of the NICE Framework. ***Within corporate environment non- government agencies often defer to OWASP or other standards created by industry rather than government.***

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 are increasingly referencing NICE framework as a tool for commercial and academic partners who rely on funding or job placement form organizations utilizing NIST or seeking a standard beyond compliance.***

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. ***Does not apply***

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. ***While we do not create certifications based on the framework, we map to it on the tail end of development as a resource for training providers. If the framework increases usability, we may alter development more aligned with framework as industry dictates.***

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. ***Does not apply***

8. Describe any tools, resources, or publications that exist that reference or would benefit by referencing the NICE Framework. ***See comments in previous section***

9. Describe any tools, resources, or technical support needed to increase the application and use of the NICE Framework. ***Would like to see a web-based tool to narrow and filter by need and mapped to resources.***

10. Propose any improvements for the application and use of the NICE Cybersecurity Workforce Framework. ***See previous questions.***

Megan Smith Branch
Chief Operating and Product Officer

3535 Winton Pl
Rochester, NY 14623
www.certnexus.com