Please see the attached comments. Feel free to reach out with any questions.

Cheers,
Marsha

Marsha J. Bennett

Information Risk Strategy and Management Organization Capability Analyst | Chevron ITC | IRSM

Houston, Texas |

Improvements to the NICE Framework 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. 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.	Work roles with associated KSATs have been very beneficial in providing standard position descriptions. Cyber roles have grown organically along with definitions of requirements for roles and what exactly the role does so having standard position descriptions will be beneficial in hiring and in transitioning people. The ability to perform all the searches (Categories/Specialty area, work roles, tasks, skills, knowledge, abilities, keywords) using DHS's NICCS Portal. The searches allow for reviewing roles with similar KSATs, identifying what roles are a good fit with certain knowledge or skill, etc. Identification of the Certifications associated with Work Roles. This helps persons understand what certifications will add value to what role. Although I cannot find this spreadsheet since the site was re-organized.
	2. Describe what components of the NICE Framework have been least useful to you and why.	There are no distinction of maturity levels for the KSATs. Our organization is large and people tend to move either laterally (broad understanding of an area) or vertically (deeper understanding of an area). The KSATs need to be broken out into maturity levels to assist in this movement.
	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 is a dire need for Operational Technology (OT)specific roles as well as where OT applies in the current roles. This area is especially important as many of our critical infrastructures in the US use Operational Technology and it's a prime target for cybercriminals. Maturity levels associated with the KSATs. We currently use four - Awareness, Fundamental, Skilled and Mastery. The KSATs need to be broken out into maturity levels to assist in this movement. See question 8. Identifying the whether skills are leadership, technical ot other type (soft skills) of skills. Again, this will assist in developing our people within our organization. Although this is Cybersecurity, IT roles are always integrated with the Cyber roles. We would like to see IT roles included. This would assist in that career pathway through ones career. We will want to identify "feeder roles" that will "supply" cybersecurity roles or cybersecurity roles that would enhance and IT role.

	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.).	The largest benefit I see is that all these audiences will be speaking the same language. Here are the bullets that we share…they may have come directly from your promotion of NICE. Sorry if I'm speaking to the choir. -Identification of critical gaps in cybersecurity staffing by employers -Improvement of position descriptions by employers -Development of curriculum, courses, seminars and research that cover the NICE KSAs and tasks by education providers -Identification of cybersecurity work Roles and specific tasks and KSAs associated with the services and hardware/software technology providers supply -Reference for cybersecurity workers to understand what KSAs and tasks employers are seeking -Reference for providers when developing training and certifications
	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.).	Benefits - again everyone is speaking same language. I would hope the formatting and frameworking would be similar. Challenges - linking frameworks makes it challenging to change one without impacting the other. Sometimes linkages become so complex that change is very difficult.
	6. Explain if you think the scope of the covered workforce as stated by the NICE Framework needs to be adjusted.	Although NICE is Cybersecurity roles, IT roles are always integrated with the Cyber roles. We would like to see IT roles included. There is a dire need for Operational Technology (OT)specific roles as well as where OT applies in the current roles. The KSATs for OT will be somewhat different as well. A SCADA system does not work like a business network.
	7. Describe any improvements that might be made in the current organization of the NICE Framework and its major components such as	See answer to question 8.

	Categories, Specialty Areas, Work Roles, Knowledge, Skills, Abilities, and Tasks.	
	8. Describe how the NICE Framework can best document and describe Knowledge, Skills, Ability, and Task statements as well as Competency Areas.	Knowledge, Skills, Ability, and Tasks (KSATs)need to be broken up into maturity levels. A new hire will not have the same KSATs as a person who has been in the cybersecurity field for 10 years. Maturity levels will help with pay scale, promotion decisions and career paths (Our organization is large and people tend to move either laterally (broad understanding of an area) or vertically (deeper understanding of an area). The definitions of skill versus ability are not very crisp and often the items in these sections seem interchangeable.
	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.	See answer to question 8.
	10. For each NICE Framework work role, please provide an informative reference that you would like the NICE Framework Resource Center to reference.	
	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	Frequent changes of a framework often make it difficult for consumption especially if the organization is working to set up a structure based on the framework. What I would like to see is a schedule of what would change and how often. That would at least allow for planning to occur. For example, Work Roles would be added (if needed) twice a year. Addition of skills might be quarterly.

	components could be managed as dynamic content (i.e., more frequent changes or updates to accommodate new information as it becomes available).	
	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.	For a large organization that develops career plans and the associated workforce management issues that come with that customization would be welcome. The Operational Technology (OT) maybe one where some roles should be kept less visible. This is just speculation on my part, I am not an SME in OT.