Thank you for giving SANS the chance to offer our suggestions for feedback and on the next round of the NICE Framework.   Please find attached to this e-mail our suggestions and thoughts. We appreciate all of the hard work the team has done in building up this initiative for the entire cybersecurity industry.   We are also glad to work with you on a discussion or to be available as a resource on the execution of our suggestions.

Brian Correia
Director of Workforce Development
\http://www.sans.org

Improvements to the NICE Framework

Thank you for giving SANS the chance to offer our suggestions for feedback and on the next round of the NICE Framework. We appreciate all of the hard work the team has done in building up this initiative for the entire cybersecurity industry. We are also glad to work with you on a discussion or to be available as a resource on the execution of our suggestions.

1. Describe what components of the NICE Framework have been most useful to you and why. **We find the number one impact that the NICE Framework has brought to the cybersecurity industry is that it has formalized work roles. The industry being in its infancy pretty much considered everyone to be a cybersecurity professional. However, as the industry has matured, we are now seeing specific skill sets and the NICE Framework has become the standard in establishing those various work roles.**

2. Describe what components of the NICE Framework have been least useful to you and why. **We find that many of the KSA's and the tasks are so detailed that they are difficult to execute on job descriptions or organizational mapping. We recommend that the KSAs and tasks be limited to the specific outcomes of the work role ID definition or that the foundational items be listed separately. An example is the Cyber Defense Analyst role which lists the knowledge of operating systems, computer algorithms, or database systems which better prepares someone for a generalist of a cybersecurity professional. By modifying the KSA's/tasks we believe it helps to solidify the position of the NICE Framework being the leader in building work roles for the industry.**

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. **We believe that the NICE Framework first off has done quite a bit of good within the cybersecurity**

industry but if all fairness it was built for the US federal government. However, as the NICE Framework expands its reach to corporate and partner nations it needs to include additional work roles outside of the government. A perfect example is a Pen Tester, a well-known job role within the industry, but is much more specific to the corporate marketplace. Just making sure these work roles are added to the next round we believe will help to make the NICE Framework more widely accepted within the entire cybersecurity industry.

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.). **We strongly believe the NICE Framework needs to focus on building resources of what are the work roles within the industry. Our belief this will only bring in more interest of the next generation of cyber professionals. It will also educate folks outside of the industry (C-Suite/HR is a perfect example) that need a place for cybersecurity 101 education. We believe it is just a natural fit for the NICE team to continue to grow as a leader on this role within the industry.**

   Expanding your scope on free resources in the marketplace will help solidify your position as a leader for folks who may not be so familiar with the industry. SANS has a ton of free resources and even hosts free classes and cyber ranges. However, many great other organizations have great resources you can reference from (ISC)^2, ISACA, CompTIA, Center for Internet Security, etc.. We can assure the NICE team we will be glad to work with you in referencing all of our resources or working with you on putting together educational materials that the community is requesting.

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.). **From a training perspective the NICE Framework has eclipsed the other initiatives when talking with federal and corporate organizations. We would like to see what can be done to better reference how all of these initiatives fit together as opposed to separate initiatives.**

6. Explain if you think the scope of the covered workforce as stated by the NICE Framework needs to be adjusted. **We are in support of the current scope and maybe our only suggestion is you may decide to include partner nations to this list and to better focus on the needs of the corporate marketplace.**

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. **We believe the pre-requisite KSAs/tasks are overrepresented in most job roles and not specific to the actual work roles. The unintended consequence of this is that training specific to a work role will often map to less than 70% of the KSAs. This will bias toward credentials that are more generalist/foundational as opposed to training that is specific to that work role. It will also mean that credentials that prepare for real world skills will not meet the list of current KSA's and tasks.**

8. Describe how the NICE Framework can best document and describe Knowledge, Skills, Ability, and Task statements as well as Competency Areas. **Having an interactive mapping tool and a spreadsheet/PDF (with links) for printing purposes. A poster format that can be placed on a wall of organizations focused on the work roles, descriptions, and competency areas. An introduction of what factors were used in the decision process such as KSA's within the framework would help to better understand the listed items.**

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. **Yes, and we believe the NICE Framework is too focused on the foundational listing of KSA's or tasks in the definition of the work role. Maybe a separate listing of more foundational knowledge could be created since today the current KSA's/tasks are not weighed.**

10. For each NICE Framework work role, please provide an informative reference that you would like the NICE Framework Resource Center to reference. **Here are the listing of the work roles we believe are missing with a big focus on Industrial Control Systems/SCADA which is completely omitted from the current framework:**

    Security Awareness & Communications Manager - Builds, maintains and measures the organizations security awareness and communications program with the goal of securing the workforce's behaviors and ultimately creating a secure culture.

    Pen Tester - This expert finds security vulnerabilities in target systems, networks, and applications in order to help enterprises improve their security. By identifying which flaws can be exploited to cause business risk, the pen tester provides crucial insights into the most pressing issues and suggests how to prioritize security resources.

    Adversary Emulation Specialist / Red Teamer - A security expert who emulates how an adversary operates using TTPs (Tactics, Techniques & Procedures). The goal is to improve how resilient the organization is versus these adversary techniques in order to prevent, detect, and respond accordingly.

Process Control Engineer / Instrument & Control Engineer - Process control engineers design, test, troubleshoot, and oversee implementation of new processes. In plants with established control systems, the engineers may design and install retrofits to existing systems and troubleshoot hardware, software, and instrument problems in a manner that also preserves the cyber integrity of the environment.

ICS/SCADA Security Engineer - Monitor and protect industrial control system environments with the goal of keeping the operational environment safe, secure, and resilient against current and emerging cyber threats.

ICS/OT Systems Engineer - Designs, builds, and supports computer systems to support the operations environment.

OT SOC Operator - Identifies, collects, examines, and preserves evidence form OT / ICS environments using controlled and documented analytical and investigative techniques that minimize the impact to the operations environment.

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). **Since the industry is ever evolving SANS recommends the opportunity for the community to update work roles once a year. We also have a belief that some of the current listings could be removed or combined especially within the oversee and govern category of work roles.**

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. **We do believe various organizations may need a customized roadmap especially in the classified world. SANS recommends that an application process be set-up with a third-party committee review to develop such customized roadmaps at least within the federal government. While SANS believes such a program would be useful in the corporate marketplace, we realize it would be tough and not quite sure of the benefits for the NICE team to take on such a project.**