Hi,

Please see attached input for the NIST NICE input.

V/R,
Al Ray, MS Cyber Defense (NSTISSI, CNSSI)
Naval Information Warfare Center (NIWC) Pacific
Security Systems, Code 4118
NAVAIR PMA-213 Landing Systems ISSE

STATEMENT of LIMITATION of AUTHORITY
You are hereby notified that I DO NOT have the authority to direct you in any way to alter your contractual obligation. Further, if the Government, as a result of the information obtained from today's discussion DOES desire to alter your requirements, changes will be issued in writing and signed by the contracting officer. You should take no action on any change unless and until you receive such a contract modification.

Semper Paratus

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST), is planning to update the NICE Cybersecurity Workforce Framework, NIST Special Publication 800-181. The public is invited to provide input by January 13, 2020, for consideration in the update.

The list of topics below covers the major areas in which NIST is considering updates. Comments received by the deadline will be incorporated to the extent practicable. The resulting draft revision to the NICE Cybersecurity Workforce Framework (NICE Framework), once completed, also will be provided to the public for further review and comment.

NIST held a public webinar titled "How You Can Influence an Update to the NICE Framework" to describe the planned updates and answer questions on December 3, 2019 at 1:00-2:00 p.m. EST. Details and a recording will be made available at nist.gov/nice/webinars.

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 niceframework@nist.gov. Please put “NICE Framework Request for Comments” in the subject line of the email.

All submissions, including attachments and other supporting materials, will become part of the public record and are subject to public disclosure. Sensitive personal information, such as account numbers or Social Security numbers, or names of other individuals, should not be included. Submissions will not be edited to remove any identifying or contact information. Do not submit confidential business information, or otherwise sensitive or protected information. All comments received in response will be made available at nist.gov/nice/framework without change or redaction, so commenters should not include information they do not wish to be posted (e.g., personal or confidential business information). Comments that contain profanity, vulgarity, threats or other inappropriate language will not be posted or considered.

Comments will be accepted until January 13, 2020.

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.

1. Describe what components of the NICE Framework have been most useful to you and why. Provides an inventory for the cybersecurity workforce, assisting in further identifying cybersecurity training and qualifications, a shared terminology between hiring managers and HR personnel (very important because HR does not have a clue). Past experience with apply for cybersecurity positions has been the communication skills between the hiring manager and HR. There has been no established communications of what is needed and what is expected. The screening process has been scanning a database for “key words” associated with the position.

2. Describe what components of the NICE Framework have been least useful to you and why. I did not see anything within NICE outlining funding for continual training and education. I also did not see anything related to who is being held responsible for the training and education of the following: HR, contracting personnel (those that might order IT equipment and devices), folks that might be involved with software and hardware that needs to be vetted. (i.e., hardware or software that may be created or involved with non-US territories and countries. I am seeing hardware and software that is purchased by acquisition with no regards to cybersecurity).
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.
    a) Management training in cybersecurity (all areas and not just management side). They need to have a good understanding of all areas of responsibility. Management often is only taught management information.
    b) Holding people responsible at all levels.
    c) General training for folks not directly related to cybersecurity personnel but acquisition, HR and folks that may come in contact with cybersecurity efforts.
    d) The general knowledge to all folks that cybersecurity may not directly dealing with a computing device (hardware/software) but all things considered in a IT or computing system or device(s). Cybersecurity deals with many areas (i.e., policies, laws, technical side, patch management, scanning and validation, continual updates, following a system from cradle to grave with funding, sustainment efforts, etc.).
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.). Engineers, programmers, system administrators, acquisition and supply personnel and leadership. Not everyone is involved with the process of ordering or maintaining software and hardware for government agencies. This needs to be addressed from the management level as well as down to personnel responsible for ordering and maintaining.
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.). Using the DoDI 8570 as guidance, will NICE take its place? I have a Master's degree in cybersecurity NICE outlines this as acceptable. Will NICE become the standard for DoD?
6. Explain if you think the scope of the covered workforce as stated by the NICE Framework needs to be adjusted. No
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. In a perfect world, cybersecurity would be assigned to one person with one job task skillset. However, we are not in a perfect world, it may be impossible for a person to have just one skillset, and as a cybersecurity person would you want that? Although a person may be assigned to a specific job or function it's very important that the person be well rounded. Who will be assigned and responsible for ensuring cybersecurity personnel are well rounded? My assumption is that this will be at the site/command level?

8. Describe how the NICE Framework can best document and describe Knowledge, Skills, Ability, and Task statements as well as Competency Areas. My guess is that this would be at the organization level to make the organizations document and track all areas and report up the chain. I would look at like FISMA reporting as annually reporting to higher authority outside the organization. This will force organizations at higher and lower levels to document and track compliance.
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. NICE framework knowledge descriptions; identify who this information is directed to? As an ISSM this would apply in all areas but most people only focus to one area. I agree that this would be great but there also needs to something listed as an answer to the Framework Knowledge statement. (I.e., Knowledge of technology that can be exploited. Knowledge of investigations, etc…). Is anyone going to answer these questions in the field? I agree that it's good to list the knowledge requirements, but who is being held responsible for a collective (correct) answer and holding everyone accountable? Is NICE going to fund training for all users or folks in the cybersecurity field?
10. For each NICE Framework work role, please provide an informative reference that you would like the NICE Framework Resource Center to reference. N/A
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). I did not see anything that should be static.
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. At the workforce level, cybersecurity should be pretty much the same. Security controls outline the processes involved with the different classification levels and what is required for each.

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. None seen so-far.
2. Describe how you or your organization was introduced to the NICE Framework. I was conducting research for training and development as an ISSM as a previous command/organization and found NICE several years back and an alternative to DoDI 8510.
3. Describe the greatest challenges and opportunities for increasing awareness and use of the NICE Framework. NICE needs to be advertised at the management level and pushed

out as a directive or instruction. Something that requires a response from the organization for compliance.

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. Nothing so-far. NICE is new to the organization.
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. Not using NICE yet.
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. Does not apply.
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. Have a government standard so that everyone can use as a baseline.
8. Describe any tools, resources, or publications that exist that reference or would benefit by referencing the NICE Framework. DoDI 8510
9. Describe any tools, resources, or technical support needed to increase the application and use of the NICE Framework.
10. Propose any improvements for the application and use of the NICE Cybersecurity Workforce Framework. I was an ISSM back in 2001 thru 2005 and there was no cybersecurity mandated certification process. When I introduced the subject of funding for ISSO that I was responsible for the response was that qualifications was a personal thing which would not be funding by the government. Later DoD funded certifications and began paying for the exams and renewals. Will the government continue to pay for exams and funding for continual certifications? I currently have a degree in cybersecurity so I do not need continual funding.