NICE Framework team,

CyberVista is pleased to submit the attached NICE Framework Request for Comments for review and consideration. Please feel free to let us know if you have any additional questions or follow up based on this submission.

Regards,
Simone

Simone Petrella
CEO, **CyberVista**

1300 17th Street North, 17th Floor
Arlington, VA 22209

CyberVista

To: National Institute of Standards and Technology, NICE
From: Simone Petrella, CEO, CyberVista
Date: January 13, 2020
RE: NICE Cybersecurity Workforce Framework Request for Comments

CyberVista is pleased to submit the following comments in response to NIST's Cybersecurity Workforce Framework Request for Comments. CyberVista is a wholly owned subsidiary of Graham Holdings Company (NYSE:GHC formerly The Washington Post Company) and sister company to, Kaplan, Inc., one of the world's largest and most diverse education providers. CyberVista is a workforce development company that helps organizations identify and fill skills gaps across their cybersecurity and cyber-enabled teams.

Improvements to the NICE Framework

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

The extensiveness of the list is incredibly specific and provides a comprehensive inventory of knowledge, skills, abilities, and task descriptions. It has been most useful when we use it to crosswalk the KSATs against training topics and modules we create so we understand where they align.

The specialty areas and associated descriptions are especially useful to organizations looking to set up and define their cybersecurity job families prior to creating individual job descriptions. The descriptions provide a broad enough encapsulation of the functional work to apply to a wide set of public and private organizations.

The work role descriptions are helpful as well, albeit to a lesser degree, in defining the generic roles that often exist within specific specialty areas. They serve as a useful starting point for the creation of job roles and families if paired with the unique requirements and job functions of the organization.

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

The extensiveness of the list is both its strength and weakness. While the list is thorough, it can be incredibly difficult to comprehend and utilize for organizations who aren't at a certain point of maturity. The defined specialty areas and work roles can serve as a useful starting point

As a workforce and training company, we are looking for ways to best teach the material that is covered in tasks and related KSATs. Through it provided a great starting point, it was not as helpful in organizing the materials for curriculum development

Some of the KSAT's are vague and not well defined. For example, K0015: Knowledge of computer algorithms.

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 framework would be greatly enhanced and useful for education and training providers if KSATs also shows dependencies/prerequisite and show different levels mastery. These will be crucial in creating not only lessons that teach to specific KSATs but also creating cybersecurity programs (degreed or not degreed).

To create effective training programs, it is crucial to know the prerequisite and dependencies for the KSA. For example, to understand firewall concepts well, it is crucials to know basic understanding of networking and data management. Therefore, if the lists of KSAs were presented in a way more akin to an organizational hierarchy

Levels of mastery will allow for much more manageable and efficient creation and delivery of the KSATs. For example, the subject of networking is so large that without knowing the level of mastery, KSAT statements would not be enough to create lessons/courses.

Given the framework contains information that applies to work roles that are found in both the public and private sector, it can be particularly confusing for the private sector

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.

It would be a huge improvement if the lists of KSATs were actually grouped by topic/subject instead of a seemingly haphazard list of skills. We recognize that they are organized in the same work role detail listing (which is helpful for job descriptions) but from a training and education standpoint, it is critical to logically group KSATs based on the overarching topic they relate to (i.e. network security) so that providers can develop a hierarchy to create scaffolded concepts that can be taught in a logical way.

One way to accomplish this and provide a flexible model that can be used by almost every stakeholder that leverages the framework is to add additional layers of data and reformat the document in a pivot table. Ths would allow users to filter and organize the depth of information in the framework according to their unique needs without forcing them to create their own "micro" models based on whether they're looking to build job descriptions, create training programs, etc.

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.

Per our response to proposed improvements, one of the areas that the framework fails to address are the KSAs that are required across all work roles within cybersecurity as a domain, the "barriers to entry" if you will. While those KSAs certainly exist in the current version, they are buried in various places and not readily or easily accessible without needing someone to review who has significant knowledge of the cybersecurity workforce or the relevant job roles the workforce fulfills.

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).

For ease of use and consistency across industries, the categories, speciality areas and work roles should change as infrequently as possible. This will allow organizations to actually review and implement a common lexicon of job definitions and roles without having to constantly cross-check updates from NICE. This is particularly important as most organizations do not regularly or routinely review and update their job role definitions or job descriptions.

Awareness, Applications, and Uses of the NICE Framework

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.

In order to create and deliver flexible and dynamic content that aligns to skill requirements and cyber career path, CyberVista created our own taxonomy of cybersecurity functional areas from subject level nested all the way down to learning objective level. We develop curricula that support cybersecurity skills development by creating programs that 1) define topics that align with NCWF tasks and KSAs, 2) start with a diagnostic assessment which provides critical team-level and personalized feedback, and 3) deliver modular learning content via extensive online resources and engaging interactive delivery tailored to the organization.

We bolster this learning pedagogy by reinforcing learning through frequent practice and reinforcement, using innovative technologies and a robust learning management system. In addition to focuses on knowledge-based outcomes, we combine hands on learning through lab-based demos, scenarios, and challenges. Each of these all map to NCWF's KSAs and are designed in a fashion that allows them to be weighted and configured based on specific organizational or job role requirements.