To Whom It May Concern:
Attached are AFPM's comments on the planned update to the NICE Cybersecurity Workforce Framework. AFPM appreciates the opportunity to provide feedback on this important initiative.

Sincerely,
Maggie O'Connell

Maggie O'Connell
Specialist, Regulatory Affairs

American
Fuel & Petrochemical
Manufacturers
1800 M Street NW
Suite 900 North
Washington, DC 20036

American
Fuel & Petrochemical
Manufacturers

1800 M Street, NW
Suite 900 North
Washington, DC 20036

afpm.org

January 13, 2020

Via niceframework@nist.gov

NICE Framework Request for Comments
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Subject: NIST Special Publication 800-181, NICE Cybersecurity Workforce Framework Request for Comments

To Whom It May Concern:

The American Fuel & Petrochemical Manufacturers Association (AFPM) appreciates this opportunity to provide comments for consideration in the planned updates to the National Institute of Standards and Technology (NIST) Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Framework).[1] AFPM is a national trade association whose members comprise virtually all U.S. refining and petrochemical manufacturing capacity. AFPM's member companies produce the gasoline, diesel, and jet fuel that drive the modern economy, as well as the chemical building blocks that are used to make millions of products that make modern life possible.

AFPM members have been at the forefront of cybersecurity efforts, participating in a wide range of industry and government initiatives to enhance cybersecurity for critical infrastructure within the oil and natural gas, and petrochemical sectors. AFPM participated in the development of the NIST *Framework for Improving Critical Infrastructure Cybersecurity* and our industry frequently utilizes NIST tools to design and implement cybersecurity risk management programs. AFPM and its members also greatly understand the need for workforce development efforts targeted to cybersecurity, recognizing that cybersecurity professionals have unique skills that are in short supply and are vital to our nation's security.

As a result of AFPM's collaborative relationship with NIST and our members' clear commitment to cybersecurity, we applaud this effort to update the Framework and welcome this opportunity to provide comments to further improve the application and use of this resource within the energy sector.

Background

Cybersecurity is unlike any other field, and in no other job market is the skills gap more pronounced. In fact, there is a predicted 350 percent growth in open cybersecurity positions from 2013 to 2021.[2] Simply put, an

[1] *See* National Institute of Standards and Technology Special Publication 800-181, "NICE Cybersecurity Workforce Framework," August 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.
[2] *See* The Herjavec Group, "The 2019 Official Annual Cybersecurity Report," October 2019, https://www.herjavecgroup.com/wp-content/uploads/2019/10/HG-CV-2019-Cybersecurity-Jobs-Report.pdf.

estimated 3.5 million jobs will be open and unfulfilled by 2021.[3] AFPM and its members recognize this concern, and actively support industry and government initiatives to build and develop an effective, versatile cybersecurity workforce. AFPM is a proud sponsor of the annual Department of Energy (DOE) Cyberforce Competition, which increases hands-on cybersecurity education specific to energy critical infrastructure to both students and professionals. Through its Workforce Development program, AFPM also serves as a conduit for members and regional partners to discuss best practices, aiming to deliver the diverse and qualified workforce needed for the entirety of our industries' operations, including cybersecurity.

AFPM supports the NICE Framework, which is an important high-level tool to identify, recruit, develop, and retain cybersecurity talent by enabling organizations to better define their cybersecurity workforce and identify gaps in staffing. The Framework underscores the interdisciplinary nature of cybersecurity, and encourages organizations to leverage these needs to build a successful cybersecurity program. It also provides tools for organizations to employ when creating position descriptions that are consistent with existing industry standards and language. Furthermore, through use of Knowledge, Skills, and Abilities (KSAs), the Framework identifies gaps in training and certification where education providers can develop curriculum around current employees or the emerging cyber workforce.

Comments

AFPM welcomes NIST's efforts to update the NICE Framework and recognizes that as cybersecurity continues to become an increasingly critical management issue, the need to embolden the cybersecurity workforce is one of the most serious economic and national security challenges we face today. Toward this end, AFPM would like to underscore the components of the Framework that have been most useful to our industries and discuss areas to improve.

Mapping Tool

The ease in which the NICE Framework can be applied to organizations seeking to fill cybersecurity positions is incredibly valuable. Utilizing a common lexicon and establishing a taxonomy of cybersecurity functions enables many industries to apply the Framework successfully. In particular, AFPM believes the NICE Framework Mapping Tool is a practical and helpful resource for managers to better define their workforce needs. The Mapping Tool helps organizations create an inventory of their existing cybersecurity personnel, so that they can more effectively plan for workforce growth. Furthermore, the Mapping Tool analyzes cybersecurity workforce needs against the NICE Framework to create a comprehensive picture of the organization's existing personnel and to easily develop specific position descriptions for current or future workforce growth using the common nomenclature.

AFPM members, many of whom are large multi-national corporations, appreciate that the Mapping Tool provides a consistent language to apply across an organization. In other words, if a company has multiple business units with different role names, the Framework position descriptions more accurately reflect the necessary position skills and duties. Additionally, AFPM members have found the Mapping Tool useful for determining additional skills and training needed within their existing cybersecurity workforce. As many vendors and educators are mapping their training and certification programs to the Framework, educational growth and career

[3] *Ibid* at 3.

development opportunities within the current and aspiring cybersecurity workforce are becoming more standardized.

Applicability to Operational Technology Operations

While the consistent language and lexicon standardized in the NICE Framework is very useful for the cybersecurity workforce in the Information Technology (IT) space, AFPM members have found it difficult to apply the Framework to their organization's Operational Technology (OT) functions. Over the past several years, manufacturers have moved from distinct IT and OT controls to more reinforced cybersecurity programs that include converged operations, with responsibility for all cybersecurity assigned to the organization's chief information security officer (CISO). Most exploits in the manufacturing space impact OT by compromising IT assets, so an organization's entire cybersecurity posture must be considered when developing a cybersecurity workforce plan. AFPM believes that refining the work roles and KSAs to take into account the unique needs of OT operations will improve the applicability of the Framework across the manufacturing sector and reinforce the merging of IT and OT cultures within the cybersecurity workforce.

New and Emerging Technology Skills

The Internet of Things, the Industrial Internet of Things, and 5G are rapidly changing how companies do business, and with rapidly changing technologies comes new vulnerabilities and risks. As written, the Framework does not account for these new technologies and the skills required to understand and mitigate the associated risks. AFPM recommends that NIST refine the KSAs to capture these new skills and consider more frequent updates to the Framework as new technologies are developed. Continually reevaluating the KSAs to take into account these critical skills will benefit not only employers, but also encourage the existing cybersecurity workforce to seek opportunities for training and education in the applicable technology.

Conclusion

AFPM thanks NIST for the opportunity to provide input on the planned updates to the Framework. AFPM supports the Framework and the thoughtful consideration NIST undertook when soliciting feedback on the updates. AFPM recognizes that cybersecurity is a dynamic and rapidly growing discipline that requires skills unmatched by any other field. By understanding those proficiencies, companies can build and develop a cybersecurity workforce tailored to their specific needs, and the Framework serves as an easily adoptable solution to achieve those goals. Nonetheless, awareness of emerging technologies and improving the KSAs to better relate to the broader operational technology space would improve the overall applicability of the Framework across the breadth of the cybersecurity workforce.

We look forward to continuing to work with NIST and other stakeholders on developing additional guidance for improving cybersecurity. If you have any questions or if AFPM can be of any assistance in this process, please contact the undersigned at (202) 457-0480 or jgunnulfsen@afpm.org.

Sincerely,

Jeffrey Gunnulfsen
Senior Director, Security & Risk Management