Request for Information

Request for Information:
The National Institute of Standards and Technology (NIST) requests information on the scope and sufficiency of efforts to educate and train the Nation's cybersecurity workforce and recommendations for ways to support and improve that workforce in both the public and private sectors.

Responses to this RFI will inform the assessment and report of the Secretaries of Commerce and Homeland Security to the President.

Reference: Executive Order

General Information:

1. **Are you involved in cybersecurity workforce education or training?**

- The US Coast Guard's training program for cybersecurity professionals is based on competencies and performance standards that align to Department of Defense (DoD) standards, which are based on the NICE (National Initiative for Cybersecurity Education) National Cybersecurity Workforce Framework (NCWF). The US Coast Guard has limited organic cybersecurity training courses and significantly leverages DoD and commercial cybersecurity training opportunities for the workforce – enlisted, officer, and civilian employees.
- The US Coast Guard complies with DoD standards regarding cybersecurity certifications.
- The US Coast Guard Academy provides a Bachelor of Science degree to graduates who are commissioned as officers. Limited cybersecurity training and education opportunities are contained within the curriculum. The US Coast Guard Academy is pursuing designation as a Department of Homeland Security and National Security Agency Center of Academic Excellence in Cyber Defense Education and will establish an accredited cyber systems major. The US Coast Guard Academy curriculum provides future Coast Guard officers with the knowledge and skills to perform some cybersecurity functions and roles.
- The Coast Guard funds postgraduate education in cybersecurity for personnel at accredited academic institutions.

Growing and Sustaining the Nation's Cybersecurity Workforce:

2. **Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?**

- Yes. The US Coast Guard workforce is categorized by enlisted, officer, and civilian employees. The US Coast Guard is implementing a cyberspace workforce framework that will align with the DoD cyberspace workforce framework. The US Coast Guard has evaluated the NIST NICE framework and has adopted the framework to align the workforce strategy to shape future training and education in cybersecurity.

3. **Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?**

- The US Coast Guard has existing policies governing cybersecurity training, and is undertaking significant effort to evaluate, develop and mature its training and education program for the cyber workforce.

5. **Which are the most effective cybersecurity education training, and workforce development programs being conducted in the United States today? What makes those programs effective? What are the goals for these programs and how are they successful in reaching their goals? Are there examples of effective/scalable cybersecurity, education, training, and workforce development?**

- The training programs provided by the DoD provide highly effective cybersecurity and cyberspace operational training. These programs provide access to unique expertise and knowledge not always available in the commercial or private sector. Commercial training and accredited educational programs are increasing in number and effectiveness as demand for quality education and training increases. Improved variety in modes of delivery, including on-line courses and self-paced training on-line training, are increasing scalability and access to cybersecurity knowledge. One example (not related to cyber) of a scalable, effective training model for common knowledge/skills across government and the private sector that may inform efforts in cyber training is the DHS training on the National Incident Management System (NIMS) Training Program, information available at https://www.fema.gov/national-incident-management-system.

6. **What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?**

- The greatest challenge is establishing authoritative, relevant national standards for cybersecurity workforce development that serve as the foundation for education and training in common knowledge and skills across government and the private sector. Additionally, access to training and education sources vary, and many are not scalable. Further, most training is focused only on development of individual skills and proficiency. Cyberspace workforce development should include realistic training in group and team settings that enable individuals to improve skills and proficiency as part of a group or team to perform cybersecurity tasks. This is essential because cybersecurity functions are performed by groups and teams.

7. **How will advances in technology or other factors affect the cybersecurity workforce needed in the future? How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems?**

- As technology advances, the tools and processes needed for cybersecurity also evolve in important ways. Cybersecurity training and education must be agile in its planning, assessment, development and delivery cycle to adapt to the speed at which technology drives change and the need to adapt. Traditional training and education methods, which typically involve time to assess, modify and update courses and curriculum. Traditional

methods should be supplemented by innovative, agile training, such as experiential self-learning and peer mentoring/training that employs on-line and crowd-sourcing to rapidly share knowledge of changing technology.

8. **What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the Nation's cybersecurity workforce, taking into account needs and trends? What steps should be taken:**

There is a continuing need for a national cybersecurity workforce framework and standards across government and the private sector. Such national standards are essential to developing a cyberspace workforce that can transition across government and the private sector to build and sustain national capability by ensuring a common language and common experience connecting cybersecurity professionals. The US Coast Guard follows an Apprentice, Journeyman, Master development process that will align to the NIST NICE framework to ensure all levels of the cybersecurity workforce are adequately trained and skilled to meet demand. Use of existing mechanisms to improve interchange with other Federal agencies and the private sector are critical to improving proficiency. For example, lateral entry/hiring from the private sector, use of fellowships/internships with the private sector, and joint duty assignments with other Federal agencies improves the proficiency of US Coast Guard cybersecurity workforce.