Cybersecurity Workforce RFI Responses

1. What current metrics and data exist for cybersecurity education, training, and workforce developments, and what improvements are needed in the collection, organization, and sharing of information about cybersecurity education, training, and workforce development programs?

> NICE and NICCS provide many metrics and data in this domain. An online national database of students pursuing and completing cybersecurity education and training starting from K-12 will be useful to track the growth of workforce. The schools, colleges, and training centers can be encouraged to submit relevant information on the trainee and the completed training.

A single US government portal for cybersecurity workforce development will be an excellent resource. Currently, the data and information are scattered on various organizations' portals. Case in point: NICE, NICCS, ATE Centers, CAE, DHS, etc. provide many valuable pieces of information, but one needs to know the URLs to get to those sites.

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

> NICE Cybersecurity Workforce Framework (NIST SP 800-181) defines seven Cybersecurity Workforce Categories. This is quite comprehensive and indicates a good understanding of the roles of the workforce. A review and update of the Work Roles and Specialty Areas every five years will be useful.

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

> Our University has been developing and updating cybersecurity policies over last several years and is making training available to selected personnel. A more broad-based externally-funded cybersecurity awareness training for all faculty and staff is needed.

4. What types of knowledge or skills do employers need or value as they build their cybersecurity workforce? Are employer expectations realistic? Why or why not? Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline? How do these types of knowledge and skills vary by role, industry, and sector, (e.g., energy vs financial sectors)?

> Hands-on skills and experience using latest tools and techniques seem to be highly valued. However, due to the nature of the evolution of the field, on the job training and continuous learning is the best way to keep the workforce up to date. Different industry sectors would like their cyber experts to have a deep domain knowledge. That is why cybersecurity needs to be included every industrial sector's appropriate education and training program. For example, smart grid security needs to be learnt by Electrical Engineering majors who already may be specializing in Power and Energy.

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 programs?

> CAE, SFS, NICE and GenCyber are the most effective education and training resources. ATE Centers are also doing a great job in developing workforce and providing online resources. The online resources they provide need to be updated on a regular basis and funding should be earmarked for that.

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

> There is a real shortage of trained cyber educators with hands-on experience. Provide summer fellowships to the interested STEM faculty at NIST or other laboratories for intensive training.

Need inexpensive access to virtual training labs (e.g., Michigan Cyber Range) with instructions for students learning different aspects of cybersecurity.

7. How will advances in technology (e.g., artificial intelligence, Internet of Things, etc.) 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 (CPS)?

> The advances in technology will continue to evolve the curricula of Computer Science, Information Technology, and Electrical/Computer Engineering. As long as Cybersecurity is included as a core knowledge area in these disciplines, graduates from these programs will be able to incorporate apply cyber defense techniques into the newer technologies.

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:

i. At the Federal level?

> Provide additional funding for “Train the Trainers”. The Trainers include K-12, community college, and four-year college teachers. Enhance funding for NICE, NICCS, ATE and CAE programs that are helping educate and train cyber workforce.

ii. At the state or local level, including school systems?

> Fund and introduce cyber awareness in the K-12 curriculum. It needs to be done with a similar thrust as is done to introduce “coding” in the school system.

iii. By the private sector, including employers?

> Partner closely with education and training organizations. Train the educators and encourage student training through internships, workshops, etc.

iv. By education and training providers?

> Prepare cyber awareness training programs at every level and present them on a regular basis.

v. By technology providers

> Incorporate cybersecurity best practices in their products and/or indicate cyber vulnerabilities.