Are you involved in cybersecurity workforce education or training (*e.g.,*curriculum-based programs)? If so, in what capacity (including, but not limited to: Community college or university faculty or administrator; official with a non-profit association focused on cybersecurity workforce needs; manufacturer or service company that relies on cybersecurity employees; cybersecurity curriculum developer; cybersecurity training institute; educator in a primary grade school; government agency that provides funding for cybersecurity education; or student or employee enrolled in a cybersecurity education or training program)?

I am a professor in information technology. Or program has four major pillars at the AS level: programming, database, networking, and cyber security. Furthermore, we offer a Certificate of Competence and a Certificate of Achievement in Information Security and Assurance. Students who want to continue their formal education, can take a third year of classes with us that push out a fifth pillar in web development and add further topics courses in cyber security, database development, virtualization, programming and other relevant topics as they come up. As we are one campus in a multi campus system, our program articulates to one of our four year institutions, UH West Oahu. There, students can pursue either a BAS in IT or ISA by taking roughly a fourth year of business management courses that provides students with a business acumen.

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?

Employment in the field is probably the number one best metric. Our goal is train students to enter the cyber workforce. Next, would probably be various industry certifications: Security+, CCNA, CEH, and so on.

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

Although we meet as a UH System regularly, we don’t all agree on where the needs are or how to meet those needs.

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

We struggle, as do many organizations, to educate our own employees and enforce best practices in cyber security. However, we are doing better and they are being enforced better.

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)?

Most of the workforce near us seem to value "critical thinking" and "ethics." They want people who can learn. They realize that no matter what students have learned, it will be obsolete tomorrow. Furthermore, they want ethical employees, people who will not try to "rob them blind." Many HR dept in companies continue to "require" a bachelor's degree for new employees though cannot say why. We graduate many very excellent students with an AS in IT with excellent cyber security skills that can contribute significantly to the workforce immediately, if only given the chance. Employers need to be more flexible in establishing MQs for positions so that people with adequate skill sets but without the BS can still be considered.

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?

What I find confusing sometimes is when there is a grant effort towards apprenticeship, which is typically fast, bootcamp stype training, but HRs that say need employees with a BS. There really seems to be a mismatch.

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

Security clearance; many students cannot get security clearance for a number of reasons that are beyond their being an existential threat to the country. There needs to be a better, clearer, career ladder in cyber security that has positions at the lower rungs that do not need clearance and then clear, low cost ways for them to get the clearance to move up.

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)?

IOT roll out has not been cyber security conscious. Manufacturing was so hell bent on rolling out products ahead of each other and trying to capture market share before the other that they did not clearly think through the cyber security risks their products presented.

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?

Continue to provide grant and other funding opportunities for education and industry to develop best practices in cyber education.

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

Education everyone (everyone who touches a computer) in best practices, especially in “social engineering.”

iii. By the private sector, including employers?

Provide low cost security options for companies of all sizes.

iv. By education and training providers?

Help educators by subsidizing their participation at cyber conferences.

v. By technology providers?

Develop stronger cyber regulations that IOT providers must adhere to before releasing a product to market.