Response by Derek Hansen, Associate Professor and Program Coordinator of the Information Technology Program at Brigham Young University. Below are responses to some of the questions identified in the RFI.

1. Are you involved in cybersecurity workforce education or training (e.g., curriculum-based programs)? If so, in what capacity?

I am a faculty member who teaches undergraduate and graduate courses related to cybersecurity and information technology at Brigham Young University in Provo, Utah. I am also our Program Coordinator and work with our other cybersecurity faculty members. I also develop and evaluate educational games and simulations designed to recruit more high school and college students into STEM fields as part of my research agenda.

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?

Our students are highly sought after by employers and regularly receive 6-figure salaries at leading companies such as Microsoft and Adobe. We have found that technical depth is a requirement, but communication and teamwork skills are what sets students apart. Unfortunately, many programs do not emphasize these elements enough, as they focus solely on the technical aspects of cybersecurity. Furthermore, we have found that our female students, some of whom excel in communication and teamwork skills, are particularly sought after as diversity in workplace is recognized by employers as being important.

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?

Our cybersecurity emphasis within the IT program at BYU has been highly successful as measured by placement statistics and salary information. A number of factors have led to this including faculty mentorship, integrating cybersecurity throughout the entire IT curriculum, lab-based work that requires students to use current technologies, a focus on learning-how-to-learn and not just teaching skills, requirements to have 200 hours of work experience prior to graduation, and a focus on communication and teamwork skills through our capstone project. While these elements work well in a high-quality university setting, they are not particularly scalable to the K-12 environment or perhaps other settings such as community colleges.
I have been working with colleagues at BYU and the University of Maryland to develop games and simulations (called “playable case studies”) designed for the K-12 setting and also appropriate for undergraduates. Such experiences allow students to feel what it’s like to be a cybersecurity professional, before having to spend years mastering the fundamentals. They can be highly motivational to a greater diversity of students, including those who do not like cybersecurity competitions. They can also be highly scalable and taught by K-12 teachers who do not have a perfect mastery of the subject, which is common.

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

Attracting a more diverse set of cybersecurity professionals, particularly female students. This needs to start in middle-school and continue through high school. Very few materials are available for K-12 teachers currently and those that do exist don’t always accurately convey the diversity of jobs in cybersecurity or the context in which the work occurs.

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)?

Cybersecurity will continue to be an issue in all areas of computing. It should not be thought of as a separate topic, among many. It is a thread that weaves through many computing topics. As such, we need to make sure that as these topics are taught there are companion materials developed that emphasize the cybersecurity elements.

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 support the development of cybersecurity educational materials, particularly those that are likely to attract female students beginning in K-12 settings. Continue to run cybersecurity competitions to raise awareness, but also provide other equally engaging, yet more collaborative and authentic cybersecurity games and simulations to attract a more diverse workforce. Continue to fund research on the effectiveness of cybersecurity education interventions.

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

Provide materials for state and local K-12 school districts that can help them start more effective cybersecurity programs within their schools.
iii. By the private sector, including employers?

*Increase the number of internship programs for high school and college students.*

iv. By education and training providers?

*Provide interactive educational experiences that give a sense of the diversity of jobs in the area of cybersecurity so students can decide if it is a good fit based on a realistic understanding of the job, not false stereotypes.*