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?

Currently, there are quite a few initiatives that are being undertaken, NIST NICE workforce framework being one of them, to create a framework for providing training and align with skills and abilities needed in industry. However, these efforts are not coordinated and correlated very well, and there is still a lack of coordinated effort between K-12, 2-year and 4-year colleges and universities, and employers (public and private) to enforce these standards and frameworks and use the metrics provided. There is a need to synchronize these efforts, and provide concise pathways to students by designing competency-based curriculum at the entire spectrum of educational institutions.

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

There is not enough understanding and agreement about these. There is a huge disconnect between the entire spectrum of educational institutions and employers about creating a concise pathway. There is a need to design competency-based curriculum and the first step is to collect skills from employers that would be used to map to a framework. NIST NICE framework provides the most useful and strategic platform for these. But efforts need to stepped up from federal agencies and provide funding to states, academic institutions, and other non-profits to engage in this work.

3. Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today and what makes them effective?

Many schools are coming up with stand-alone cybersecurity degrees, both at undergraduate and graduate levels, independent of Computer Science degrees. This is a positive trend. There is a need to detach cybersecurity education and degree programs from traditional computer science degree programs. Collaborative work between 2-year and 4-year colleges need to be stepped up in creating 2 year and 4 year degree programs together (competency-based curriculum design is needed), and give students opportunities to degree completion pathways. Certifications are definitely value-added. NSF's CyberCorps: Scholarship for Service and NSA's GenCyber programs are very good initiatives, and they should be enhanced with more funding.

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

More funding is needed to provide education and training. Funding levels should be enhanced from both federal and state levels.

5. What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the nation's cybersecurity workforce?

NSF's CyberCorps: Scholarship for Service and NSA's GenCyber programs are very good initiatives, and they should be enhanced with more funding. Colleges and universities should be encouraged to work more closely with 2-year colleges to design curriculum and create pathways.