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?

I do not think we have many current metrics at all. Furthermore, a metric is only useful if it is meant to indicate the status or progress of something. So, in my opinion, prior to conceiving metrics, we need to know what about cybersecurity education, training, and workforce development we need metrics for. I could see both demand and supply questions. On the demand side…..Are we trying to report the workforce shortage (quantitatively and qualitatively)? Are we trying to specify change in the nature and magnitude of the shortage? On the supply side, are we trying to measure and report a) the number of educational institutions with cybersecurity programs, b) the number of programs in existence at these institutions, c) growth in the number of institutions or programs over the past 5-10-15 years, d) the number of students enrolled in these various programs, e) the number of graduates from these various programs, f) enrollment and graduation growth over the past x-y-z years? All of these questions are answerable and *could* lead to the development of valid metrics, but it all starts with asking the right questions.

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

In my opinion, yes. The NCWF does a good job for me as an educator. I realize that hiring entities might feel differently, but from where I sit in the world, I think what we have is sufficient.

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

This is not applicable to me.

1. What types of knowledge or skills do employers need or value as they build their cybersecurity workforce? Are employer expectations realistic?

I don't feel I have anything useful to add to this.

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

What makes a program effective is it's ability to produce deep understanding among its graduates. Once a program delivers QUALITY education, then I think it can shift its focus to producing quantities.

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

I am not sure about the challenges facing employers, but the biggest challenges facing me and my institution is fighting for faculty and other resources needed to 1) start and 2) expand a cybersecurityprogram. I feel we have grown BS and AAS programs fairly noticably the past 15 years, but now we need to continue to focus on the ends, I.e, K-12 and PhD. We both need a big feeder pipeline, as in we need hundresd of thousands of K-12 students exposed. And then at the high end, we also need to increase the number of true experts to at least hundreads graduating per year.

There are many efforts underway to address these challenges. E.g., CAE, SFS, GenCyber, NICE, etc. We need to continue them and bolster them.