Good afternoon,

Below are a few comments in reference to the NICE Framework.

The authors emphasized the importance of cybersecurity education, training, and credentialing, in which UMGC clearly participates. UMGC's cybersecurity programs directly support the cybersecurity workforce development as these programs provide a broad perspective of all aspects of cybersecurity. Although NICE is geared toward the government agencies, the Framework can (with great success) be applied to non-government environments.

One of the claims the authors make is the NICE's usefulness in describing all cybersecurity related work, which may be an overstatement. Whereas in the government environment the duties of cybersecurity professionals are well-defined, smaller entities often rely on more 'generic' IT staff when ensuring their data / networks remain safe. However, one could argue that even private entities needs to employ dedicated cybersecurity professionals.

In paragraph 1.3.3 Educators/Trainers the authors charge us [as educators] with the development of appropriate curricula (degree programs) that cover the knowledge, skills and abilities (KSAs) for the cybersecurity workforce, which is precisely what UMGC does. Although the authors define what the KSAs are, it would be useful to have a list of what specifically these KSAs are (as opposed to providing general definitions). The same goes for competencies (para 4.1.). As educators, we directly support the NICE Strategic Goal #3 (Career Development) as many of our students already work in the field of cybersecurity. In fact, our cybersecurity programs (at least to a degree) touch upon all of the elements/categories outlined in Tables 1-3 (Appendix A).

In Appendix C (DHS Cybersecurity Workforce Development Toolkit) a link to the Toolkit [16-page pdf file] is provided, which is another high-level theoretical document, without much specificity. A document with more of a hands-on information would be helpful.

In summary, consistent with its name, NIST Special Publication 800-181 provides a high-level framework aimed at recruiting, developing, and retaining cybersecurity talent. Its authors have compiled a lot of information relevant especially to the government organizations. However, the document's usefulness is limited as aside from providing definition of the key terms, it does not explain what specifically they entail. Explaining these terms and (if possible) providing examples would render the document more valuable. The authors also emphasized the importance of education,

which is precisely what UMGC's Cybersecurity Programs are designed to accomplish.

Yurek K Hinz, Ph.D.

Adjunct Professor teaching Graduate courses in Cybersecurity at UMGC.