Danielle, Thank you for the opportunity to respond. Here are my initial comments. I am happy to discuss further.

The current NICE Cybersecurity Workforce Framework provides a very detailed taxonomy of envisioned roles, role specialties and candidates skills.

My observations about the current document are...
(1) This document serves an important, but limited function. As stated in 1.3 Audience and Users, the document is a "non-prescriptive cybersecurity workforce dictionary" for HR departments and staffing agencies.
(2) I can confirm that the document is not something that I would use in my prior roles as: software engineer or technical executive for security in development at a global company, or, my current role in academia as adjunct professor where I build and deliver cybersecurity education for both computer science and business track undergraduates.

Some characteristics of documents that would be more helpful for all...
(a) a description of real world organizational personas along with their roles/responsibilities for cybersecurity (rather than a list of cybersecurity roles and responsibilities that may or may not be directly mapped to organizational roles)

- *executives: strategic plan, to include cybersecurity security, establish policies, review compliance, risk management, etc. SWOT, CSF*
- *business & line managers: implement policies, measure compliance, situational awareness, risk assessment, etc. SWOT, OODA, CSF*
- *system designers, software engineers, red teams: build, integrate, test, deploy with attention to security SDLC*
- *IT operations personnel: monitor, detect, respond, recover MAPE, CSF*

(b) a description of core cybersecurity skills for each real world organizational personal that creates more well-rounded adaptable workforce (rather than lists of targeted and nuanced skills that drive specialization and fragmentation of the workforce)

- *executives: business level risk analysis, risk aware strategic planning*
- *business & line managers: business risk assessment, risk aware business planning*
- *system designers, software engineers, red teams: technical risk assessment, supply chain evaluation, adversarial thinking, assurance*
- *IT operations personnel: incident management and recovery*

(c) a roadmap of role and skill education that builds a common core of knowledge and extensions (rather than separate education that creates an isolated workforce)

- *executive and business manager: Cyber thinking, Cyber enterprises, Internet Business Apps & Services, Internet Business Risks, Supply Chain*

- *system designers, software engineers, red teams: Cyber thinking, Cyber enterprises, Internet Business Apps & Services, Supply Chain, Adversarial Thinking, Attackers and Attacks*
- *IT operations personnel: Cyber thinking, Cyber enterprises, Adversarial Thinking, Attackers and Attacks, Incident Response*

Lastly, my opinion is that everyone, including business executives, IT professionals, Educators and the general public is suffering from document overload. The idea of using Data Science and Computer Systems to gather, organize and present publicly available information in an actionable format is long overdue.

Respectfully,
Jim Whitmore
Google Scholar
Profile: https://scholar.google.com/citations?hl=en&user=gvyc14EAAAAJ