Good afternoon;
Attached are review comments for NIST SP 800-181,NICE Framework from employees at Lockheed Martin.
If you have any questions, please feel free to reach out.

Margee Herring
Information Assurance Engineer Stf - Cybersecurity
Lockheed Martin, Aeronautics
Advanced Development Programs
Ft. Worth, TX

#	Organization Name	Submitted By	Type*	Section / Page #	Comment (Include rationale for comment)	Suggested change
1	LM		G	General comment, Appendix A	This framework seemingly subsumes all aspects of IT - from legal governance to traditional programming (ref: categories SP/DEV, OV/LGA). By this definition, front-end web developers are part of the cyber workforce as are lawyers - in other words, where does it end? If nearly every aspect of an organization is subsumed into a 'cyber workforce', the meaning of 'cyber' becomes even more opaque, which runs counter to the objectives of this framework.	This document should specify ***concrete*** deliniations (if any) between cyber, IT, programming, and database work.
2	LM		G	Ch4 pp19	Future extensions to NICE - include additional context for how NICE could be extended to consider behaviors, academic, and workplace competencies.	For example, indicate that academic backgrounds in computer science are conduits for a robust cyber workforce.
3	LM		T	Ch4 pp19	Future extensions to NICE - the document indicates that, in the future, job titles should be created. Is this not already the intent of KSA ID titles?	Define the difference between KSA ID title (e.g., Cyber Crime Investigator (IN-INV-001)), and the idea of standardized job titles.
4	LM		T	Appendix A.1	Unclear difference between PR (Protect and Defend) and AN (Analyze), based on descriptions. Additionally, the term "cybersecurity information" is vague. Similarly, without looking at KSAs, the IN (Investigative) category is extremely close to the AN category.	Define the term "cybersecurity information" within the category definition of Analyze (AN). Clearly

5	LM		T	Appendix A.1	The incident response (CIR) specialty area should fall within the investigative category, not the PR category, as IR is by definition an investigation. IR cannot occur without investigating and analyzing the cause of an incident.	Move the CIR specialty area to AN.
6	LM		T	KSA/S0241	"Gisting" should be replaced as it is unclear.	Use "analyze" or "summarize".
7	LM		T	KSA/S0214	"Accessess" does not make sense in the context of the KSA.	Rewrite KSA, perhaps to: "Skill in determining value of given intelligence."
8	LM		T	KSA/S0177	Redundant with S0178.	Combine with S0178
9	LM		G	KSA/S0151	Troubleshooting failed "components" does not equate to "servers".	Components should refer to smaller scaled devices, not entire servers. Or, rephrase to say "Troubleshooting failed servers."
10	LM		T	KSA/S0255	Redundant with S0208; consider combining with S0287.	Remove S0255.
11	LM		T	KSA/S0198	Redundant with S0197.	Remove S0198.
12	LM		T	KSA/S0299	Geolocation is not part of network target analysis, unless this refers to RF-based direction finding.	Geophysical location should be removed from this list
13	LM		T	KSA/S0302	"Effectiveness" does not make sense in this context.	Rewrite for clarity.
14	LM		T	KSA/S0301	Redundant with S0203.	Remove S0301.
15	LM		G	KSA/S0304->KSA/S0353	Standardize verbiage in order to increase readability of this document.	Rewrite "Skill to" to "Skill in", which will match the format of other KSAs.
16	LM		T	KSA/K0274	WiFi does not stand for "Wireless Fidelity".	Remove definition of "WiFi"
17	LM		T	KSA/K0375	Redundant with K0274.	Remove K0274.
18	LM		T	KSA/S0241	Do not explicate specific tools in KSAs. Tools are ephemeral by nature and do not fit within the context of a framework.	Remove mention of the 'traceroute' program.

19	LM		E	Abstract/ii	Might want to mention how the National Cyber Strategy and the White House Strategy mentioned about workforce development, and how this NICE framework fits in.	
20	LM		E	Introduction/1	The intro section focuses a little too much on IT. Should we try to look at other aspects of cyber like information assurance, architectural analysis, network analysis, etc.? What about EW or RF spectrum in general? Or IT and OT like ICS systems or SCADA systems? So, when they say "integrated" in the doc, it shouldn't be just about technical and non-technical roles, but should be encompassing the aforementioned disciplines because inherently, the word "cyber" is so broad	
21	LM		T	1.3.1/3	Employers should not just define the career paths, but they themselves should be developing a technology roadmap (or reference one from the industry) and explain how the career paths could fit into the roadmap	Either add a new bullet or elaborate on the bullet #4
22	LM		E	4.1/10	Might want to include ethics in one of the core competencies; many times it's not the hackers sitting across the globe that are doing the most damage; it's actually the insider threats that are most difficult to spot and mitigate—hence the whole zero trust model.	

23	LM		T	Task Description/30	Between T0162 and T0164, we might want to explore integrity associated with data at rest and data in transit. T0162 seems to imply that we need to focus on data integrity in a database. But, what if data isn't stored in a database?	
24	LM		T		I don't think I have seen "Red Teaming"; the list does have penetration test, though.	
25	LM		T	KSA Description/59	What about data analytics like using AI/ML/DL for cyber analysis purposes? There is data mining and data warehousing	
26	LM		T	KSA Description/60	K0032 cyber resiliency and redundancy have some overlaps	I'd recommend breaking resiliency out further—in terms of withstand, mitigation and recovery. Redundancy is one of the enabling technologies or techniques to allow recovery.
27	LM		G	Securely Provision/95-122	Good job at combing KSAs, tasks, etc together; very useful for job specification	

28	LM		E	General	"Systems security engineering is a specialty engineering discipline of systems engineering that applies scientific, mathematical, engineering, and measurement principles, concepts, and methods to coordinate, orchestrate, and direct the activities of various security engineering specialties and other contributing engineering specialties to provide a fully integrated, system-level perspective of system security."	Systems security engineering is inclusive of Requirements Engineering as defined by ISO/IEC/IEEE 29148:2018(E) Systems and software engineering – Life cycle processes – Requirements engineering. NIST SP 800-160v1 defines system security requirements as "System requirements that have security relevance. System security requirements define the protection capabilities provided by the system, the performance and behavioral characteristics exhibited by the system, and the evidence used to determine that the system security requirements have been satisfied. Note: Each system security requirement is expressed in a manner that makes verification possible via analysis, observation, test, inspection, measurement, or other defined and achievable means." The Systems Security Engineer is the "Individual that performs any or all of the activities defined by the systems security engineering process, regardless of their formal title. Additionally, the term systems security engineer refers to multiple individuals operating on the same team or cooperating teams." The NIST focus on Engineering via NIST SP 800-160v1 is an important aspect of the Securely Provision (SP) category, and is deserving of its own Specialty Area, Systems Security Engineering (SSE). Systems Security Engineering (SSE) is clearly a necessary area to Securely Provision (SP). In addition, we see that (ISC)2 is also focused on the SSE by how they have adjusted the standards for the ISSEP concentration within the CISSP discipline to also mirror NIST SP 800-160v1. We also note that Technology R&D (TRD), Systems Requirements Planning (SRP), Test and Evaluation (TST) and System Development (SYS) are all sub-specialty areas to the Systems Security Engineer/Engineering (SSE).

						It is also of note that DoD recognized that the IASAE (DoD 8570.01-M) are separate but equal Specialty Areas. The Level III IASAE requires an ISSAP or ISSEP. One would expect the NICE Framework to acknowledge this point. As my signature illustrates, I am a CISSP-ISSEP and an ESEP (among others). It takes an Systems Security Engineer to assure the technical solution is correct for Cybersecurity.