Bill and Ken:

Here are my comments on draft NIST Special Publication 800-181 - National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Please let me know if a word document is a no-no and what format you would prefer.

Thank you.
Walt

Comments on NIST Special Publication 800-181 - National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework by Walter Houser at walthouser@gmail.com

2 NICE Framework Components and Relationships

2.1.2 In previous versions of the NICE Framework, tasks and KSAs were associated with each specialty area. KSAs and Tasks are now associated with the work roles. An explanation of why this change was made would help the reader understand the framework and how it has developed to meet organizations' requirements.

2.1.4 Please clarify the distinction between skills and abilities. At a superficial level abilities are natural or inbuilt while skills are learned behaviors. However, the boundary is fluid, perhaps even arbitrary; the assignment of a concept as an ability versus a skill is typically influenced by one's viewpoint on the dichotomy between nurture versus nature. No one is born with the abilities listed in Appendix A.7 for example "A0005: Ability to decrypt digital data collections." In my opinion this distinction is an unhelpful distraction and should be avoided by combining the list.

3 Using the NICE Framework

3.2 "Position descriptions and vacancy announcements using the NICE Framework terminology support more consistent evaluation criteria for vetting and approving candidates." Unfortunately employers often issue recruitment descriptions for an entry level position that require skills implying a decade of experience. How could the framework mitigate this risk? Involving the first line supervisor at multiple points in the PD process is one method of reducing this risk.

3.4 "The NICE Framework is helpful for existing employees who desire to move into a cybersecurity work role from another position. An organization can describe the KSAs needed to allow a reliable employee in a non-cybersecurity work role to become part of the cybersecurity workforce taking on cybersecurity tasks." Please clarify how could the framework be used to facilitate workforce retraining?

Appendix A – Listing of NICE Framework Elements

A.1 Tables 4, 5, 6, 7 and Appendix B should be derived from the Reference Spreadsheet for NIST Special Publication 800-181, and any discrepancies resolved in favor of the spreadsheet.

A.1 Where is Supply Chain Management in Appendix A? The following tasks and KSAs explicitly address supply chain risk management:

Sheet	Name	Cell	Value
Master KSA List		B130	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)
Master KSA List		B152	Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supply chain risk.
Master KSA List		B158	Knowledge of supply chain risk management standards, processes, and practices.
Master KSA List		B173	Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.
Master KSA List		B268	Knowledge of program protection planning (e.g. information technology (IT) supply chain security/risk management policies, anti-tampering techniques, and requirements).
Master KSA List		B1009	Skill to ensure that accountability information is collected for information system and information and communications technology supply chain infrastructure components.
Master KSA List		B1021	Ability to apply supply chain risk management standards.
Master Task List		B202	Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.
Master Task List		B259	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.
Master Task List		B276	Develop and document supply chain risks for critical system elements, as appropriate.
Master Task List		B279	Participate in the acquisition process as necessary, following appropriate supply chain risk management practices.
Master Task List		B305	Develop contract language to ensure supply chain, system, network, and operational security are met.
Master Task List		B417	Develop supply chain, system, network, performance, and cybersecurity requirements.
Master Task List		B418	Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered.
Master Task List		B528	Provide enterprise cybersecurity and supply chain risk management guidance.
Master Task List		B554	Draft and publish supply chain security and risk management documents.
Master Task List		B555	Review and approve a supply chain security/risk management policy.

However, the categories and specialty areas they apply to are not clear. Is SCRM spread so widely across the framework that calling out SCRM in the categories and specialty areas would be unduly repetitive? The problem with this arises when an organization wants to establish a SCRM program and needs to write the position descriptions and recruit the required personnel.

A.1 Table 1 Agile development and DevSecOps would appear to straddle SP and OM. As with SCRM, a manager of an agile or scrum program would likely see the NICE categories as ill-suited to their needs. This condition is particularly acute with the advent of containerization, with DevSecOps teams deploying infrastructure as code.

A.2 Table 2 Legal Advice and Advocacy (LGA) should include 1) protection of intellectual property rights, and 2) selection and management of licenses appropriate to the code source. Failure to appreciate these tasks can lead to vulnerabilities, lack of accountability, and litigation.

A.2 Table 2 Collect and Operate (CO) category should be dropped. Collection Operations and Cyber Operational Planning should move to the OM category.

A.2 Table 2 Cyber Operations (OPS) should be renamed Cyber Intelligence. The term “operations” is generally understood to relate to Operate and Maintain (OM). Cyber Intelligence (vice Cyber Operations) should go to the Analyze (AN) category, possibly folded into Threat Analysis (TWA).

A.2 Table 2 There is a lot of overlap between categories Analyze (AN) and Investigate (IN). Perhaps the two categories could be combined, and the specialty areas realigned.

A.2 Table 3 should be populated with more references from CNSSI 4009 and NIST SP. For example, contact Dr. Paul Black for citations in the DEV category.

A.4 Table 3 The Authorizing Official/Designating Representative should be a business manager not technical manager. Please add to the Authorizing Official (SP-RSK-001) role (1) the task of weighing risk to business outcomes with the cost of controls. This role should also have (2) the task of identifying and evaluating risks to the business. Furthermore, the AO should have (3) the task of managing the resources needed to address this risk. This role should also have (4) the responsibility to ensure IT solutions reflect the organization’s overall risk appetite.

Appendix B – Work Role Detail Listing

Appendix B should identify the NICE Framework Tasks (or their combination) required for performance at each level of proficiency (beginner, intermediate, and senior/expert).

Appendix C – Workforce Development Tools

Appendix C. The DHS Cyberskills Management Support Initiative PushbuttonPD Tool should be generated from the Reference Spreadsheet for NIST Special Publication 800-181.

Appendix D – Cross Reference to Guidance and Guideline Documents

D.1 The NICE Framework does not match nor smoothly align with the NIST CyberSecurity Framework. Consideration should be given in the long term to realigning NICE to the CSF.

D. It would be helpful for NIST SP 800-53 control families to align as well. Thus organizations could identify the KSAs needed to implement a given control. This capability would facilitate the recruitment and acquisition of personnel and providers to implement security controls.

Questions perhaps tangential to the NICE Framework

What are essential characteristics of a good security personnel program?

What are the characteristics of successive improvements in such a program?

How would a maturity model for the NICE Framework guide organizations seeking to improve their security personnel practices?

What would be the possible parameters of such a security personnel program?