National Cybersecurity Workforce Framework

Comments on Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"

Part I - Request for Information

General Information

Question	Comment	Severity	References
Are you involved in cybersecurity workforce education or training (e.g., curriculum-based programs)? If so, in what capacity (including, but not limited to: Community college or university faculty or administrator; official with a non-profit association focused on cybersecurity workforce needs; manufacturer or service company that relies on cybersecurity employees; cybersecurity curriculum developer; cybersecurity training institute; educator in a primary grade school; government agency that provides funding for cybersecurity education; or student or employee enrolled in a cybersecurity education or training program)? *Note:* Providing detailed information, including your specific affiliation is optional and will be made publicly available. Commenters should not include information they do not wish to be posted (e.g., personal or confidential business information) and are strongly encouraged not to include Personally Identifiable Information in their submissions.	No. N/A		

Growing and Sustaining the Nation's Cybersecurity Workforce

Question	Comment	Severity	References
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?	Metrics and data on cybersecurity education are limited to mandatory annual Cybersecurity (Information Assurance) Awareness training only. No metrics or data currently exists for the agency Cybersecurity Workforce roles, including (a) cybersecurity education, (b) training, and (c) workforce development.	Critical	
2. Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?	No. Agency leadership does not understand workforce categories, specialty areas, work roles, or knowledge/skills/abilities related to the Cybersecurity Workforce Framework.	Critical	
3. Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?	No. Agency leadership categorically denies training other than to "Continuing Legal Education" for support personnel in other workforce roles, including the Cybersecurity Workforce without exceptional circumstances.	Critical	
4. What types of knowledge or skills do employers need or value as they build their cybersecurity workforce? Are employer expectations realistic? Why or why not? Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline? How do these types of knowledge and skills vary by role, industry, and sector, (e.g., energy vs financial sectors)?	The agency requires positions with knowledge, skills, and abilities across the Cybersecurity Workforce, however none of these KSAs are valued, nurtured, maintained, or grown. No. The agency leadership assigns work inconsistent with or inappropriate for Cybersecurity Workforce categories, specialty areas, work roles, and KSAs. As an example, Leadership assigns database conversion/entry duties to Cybercrime Investigator work roles and computer forensic duties to Application Support work roles; and additionally denies training to learn the required skills.	Cittical	

5. Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today? What makes those programs effective? What are the goals for these programs and how are they successful in reaching their goals? Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs?	The Defense Cybercrime Center (DC3)/Defense Cyber Investigations Training Academy (DCITA) provides a diverse, comprehensive, and effective set of knowledge, skills, and abilities as well as practical application for the NCWF Investigate category. This program is progressive and combines lecture, reading, demonstration, and practical application with a comprehensive written and practical exercise at each stage ensuring skills competency in the NCWF category sufficient to begin work immediately with little or no supervision. The goals of the program are to provide the KSAs and practical experience required to perform work in the Digital Forensics or Investigation specialty areas, along with an accredited certification program. For the DC3/DCITA programs, the progressive certifications offered are for a Digital Media Collector that maps to certain Digital Forensics or Incident Responder work roles, Digital Forensic Examiner that maps to Digital Forensics or Defensive Digital Forensics work roles, and the Computer Crime Investigator that maps to the Investigation work role. This instruction is both progressive and scalable, as well as flexible in its instruction to incorporate appropriate tools and methods as they develop over time or are impacted by changing legal prescendent.	Administrative	http://www.dcita.edu http://www.dc3.mil
6. What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?	(a) The Nation: As a result of recission of the Federal Human Resources Manual, there is lack of directive policy on providing career sustainment and career development training for agency support personnel under 5 U.S.C. § 4101 et seq. and 5 C.F.R § 410. Training and career development in the federal workforce is seen as a favor to the employees rather than a required business acitivity to sustain the workforce. This is especially true of technology training programs that are often longer and more expensive than other career sustainment and workforce development training programs. The result is that "corporate knowledge" stagnates and atrophies or skilled and productive workers self-fund training and then seek to recoup that cost through other employment. (b) Employers: Similar to (a) above, Employers must take action to invest in their workforce or face the same atrophy/exidous of corporate knowledge. (c) Lack of sustainment training, meaningful career progression, and supportive career development opportunities degrades employee morale and loyalty, as well as diminishes the productivity of the workforce over time.	Critical	
7. How will advances in technology (e.g., artificial intelligence, Internet of Things, etc.) or other factors affect the cybersecurity workforce needed in the future? How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems (CPS)?	No comment. No comment.	N/A	

8. What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the Nation's cybersecurity workforce, taking into account needs and trends? What steps should be taken: i. At the Federal level? ii. At the state or local level, including school systems? iii. By the private sector, including employers? iv. By education and training providers? v. By technology providers?	i. A reintroduction of the Federal Human Resources Manual that addresses training, or additional policy to provide career sustainment and career development training and education that is relevant to the work role. Without these nurturing programs, there is very little incentive for new technologists to enter the federal workforce, and for existing technologists to continue unless they are simply willing to stagnate until retirement. Civil service, even as a pathway to obtaining cybersecurity workforce education and experience should considered beneficial to national security, even if the federal employee leaves for commercial/private employment. The fear of creating revolving door training programs where an employee enters the workforce and then leaves shortly after obtaining training and basic experience should be seen as beneficial to the United States cybersecurity workforce health. ii. State and local schools are already incorporating advanced computer, and technology career education and exploratory programs. Some high schools include previously collegate-level programming, robotics, and computer science courses. This should be encouraged, however should be supplemented with ethics courses to prevent creating a generation of "hackers". iii. Education regarding information technology categories, specialty areas, and work roles should be promulgated to the private sector. Many job annoucements at the all evels from entry to senior require such a diverse set of skills that an employee would either fail, expect/demand a much higher salary than	Serious	