National Cybersecurity Workforce Framework, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"

Comments on Executive Order 13800,

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	Yes, I am. Bay de Noc Community College, Computer Network Systems and Security Instructor.		https://www.iad.gov/NIETP/reports/current_iace_certified_institutions.cfm#M

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 currently exist through the NSA IACE Courseware Evaluation program. Many of the certified institutions currently work with K12 schools and ISDs to dissiminate cybersecurity education, training, instruction as part of articulation program. This is an optimal structure to begin working from to further enhance cybereducation. Improvements could include coordination of regional training and seminars (leverage Infragard members) to provide training for instructors to bring back to institutions and K12 institutions through articulations.	Medium	https://www.iad.gov/NIETP/reports/current_iace_certified_institutions.cfm#M
2. Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?	No. Many educational leaders lack basic understanding of the issue. Often it is confused with "Knowing how to create a strong password" or "Compliance related issues". Significant dissemination to K12 and higher education leadership should be conducted to increase knowledge of cybersecurity workforce categories, specialty areas, work roles, or knowledge/skills/abilities.	Medium	
3. Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?	Yes. I confident that my institution of higher eductation, specifically IT leadership, understands and has implemented the necessary policies, processes and procedures to secure our data and systems. However, there are scores of reminders both locally and nation wide that training most continue.	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)?	It is critical that employers become more knowledgeable of the need for Cybersecurity workforce categories so that fix the problem using the correct tool. Many employers are still under the impression that a "blackbox solution" or a "cyberhacker" will provide them a silver bullet solution. This just is not so. No, employer expectations are not realistic as evidenced by recent job postings for "security compliance", certified ethical hackers, and backup and redundancy systems specialists. The answer is not fill these specialized roles until there is a systemic game plan in place. Absolutely not! There exists a huge knowledge gap in employers that must be plugged prior to or possibly simaultaneously addressing the lack of qualified IT specialists. Mostly in application to the specialized hardware and software encountered in these sectors. However, the good news is that this is not an insurmountable issue as long a team effort is coordinated.	Critical	https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

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?	NIETP NSA IACE Courseware Evaluation standards have been availble since 2000 and have proven to be exception if implemented in curriculum. What makes the NIETP NSA IACE Courseware is that it is excellent for all levels of education and allows for great flexibility to be used to educate both employers and general public if implemented correctly. Once mapped to the NIETP NSA IACE Courseware, instituions have been certified for 5 years. All that must be done is add goals to expand it on an annual basis.	Medium	https://www.iad.gov/NIETP/reports/current_iace_certified_institutions.cfm#M
6. What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?	(a) Becoming stuck in quicksand and not doing anything (b) Excpecting all students to succeed at higher level math and higher order programming languages, neither of which are required for them to be successful in cybersecurity. We need to work on our existing strengths, increase community college instructor skillsets, and educate employers.	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)?	I expect advances of technology to speed up "bad actors" ability to compromise systems. This will most likely mean that new software and systems will need to be implemented that can respond in far quicker time than humans. However, our workforce must always be 'smarter than the box' when it comes to implemenation, monitoring and response. That is where cybersecurity education, training, and workforce development programs come into play. In terms of how much cybersecurity education, training, and workforce development programs need to adapt, it just plain depends on the program. Most have a good start, and just need some guidance to be productive and useful.	Medium	

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. Implement guidance and monies to further strengthen community college instructors in new technologies. Many existing dollars (Perkins, NSF, etc…) have been siphoned off to support inadequately prepared students. Stengthen existing funding streams and institute new policies that will not allow dollars to be siphoned off. ii. Work with local educational advisory groups and workforce development boards to survey employers through gap analyis to determine regional weaknesses and then to coordinate which institutions should strenghten or develop new training programs. Then, by strengthening articulations (K12 to community college, and community college to university) to develop dissemination channels. Finally, leverage experts from all levels (coordinated with Infragard) to push dissemination to employers and general public. iii. infragard is an excellent place to start! iv. Education and training providers must strengthen instructor skills by assisting instructors to attend training. Funding streams (Perkins, i.e.) have been drying up for over a decade. v. Webcasts and seminars are helpful.	Medium	