General Information

1. 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 Start Printed Page 32174funding 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.

Response: Deputy Communications Officer for Information Systems Security Association (ISSA) in Colorado Springs, CO. ISSA is an international non-profit organization of information security professionals and practitioners.

Growing and Sustaining the Nation's Cybersecurity Workforce

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?

Response:

My own cybersecurity knowledge has been acquired primarily through years spent as a NSA government employee, working in the Information Assurance Directorate. NSA recognizes colleges as National Centers of Academic Excellence (in cyber) and have Senior Executives responsible for interfacing with particular schools to assure they continue to meet standards and maintain accreditation. Within this program, metrics are measured.

Regarding improvements, I believe there should be one body that "owns" cybersecurity certification for the public, non-DoD community. While there are several common certifications, such as CPA, EIT, etc, and various avenues like ICS2, CompTia, CISCO, etc., there is no single, definitive path to take, or goal to meet for aspiring cybersecurity experts. There needs to be one widely recognized and centralized location/mechanism to oversee cyber certification and accreditation, metrics, information sharing, etc.. Perhaps a model similar to the way CPA's are tested and certified can be used in the emerging cybersecurity realm.

2. Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?

Response:

No, I do not believe there is sufficient understanding. Just by looking at the cyber job ads, I notice there are inconsistencies in what employers are looking for and how that translates to various levels - entry, junior, and senior cyber professionals. Too often, I see job vacancy ads where companies are looking for senior level professionals, but when I read the detailed work descriptions they sound more like junior, or even entry-level.

In addition, the focus almost always seems to be on detect and protect, i.e., taking a proactive/tactical approach. What I see missing is the understanding of the need to do more strategic, architectural planning and execution. It seems, too, that there is not a lot of emphasis and/or educational avenues for the non-hands-on aspects of cyber (e.g., architecture development, RMF documentation, CVE risk analysis and evaluation, etc.). An emphasis on "Capture the Flag" is understandable because it can be fun and exciting, but the behind the scenes, non-hands-on work necessary for proper design and accreditation is just as important.

3. Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?

Response:

No, I am not seeing appropriate cybersecurity policies in place at the small/medium business level or even at local doctor's offices, banks, supermarkets, etc. It is also my experience that most large organizations do have these kinds of policies in place, but it is frequently left up to their employees to read, understand, and implement the policies on their own time and at their own initiative. What enforcement I have seen for cybersecurity policy has traditionally been through the organization's ISSO or IT staff, which limits the scope and asks too much of the IT people. Lots of people don't understand the difference between IT and cybersecurity. On the positive side, though, I will give a plug to the CyberSecurity Framework as a good foundational document that provides a basis for evaluating and making risk decisions.

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)?

•What types of knowledge or skills do employers need or value as they build their cybersecurity workforce?

Response: Although Cybersecurity/Information Assurance, as a specialty, has been around for a long time, it is only recently, with the advance of technology and "Internet of Things" where it has now become a recognized and necessary skill set in the workplace. The problem, though, is there is not sufficient buy-in/recognition of cybersecurity at the senior executive level. It can only be successfully implemented, I believe, when an organization places cybersecurity on par with other business units like HR, Recruiting, Accounting, etc. Simply asking a company's IT department to handle cybersecurity is not a reasonable approach, but it's one that many companies keep trying to do.

•Are employer expectations realistic? Why or why not?

Response: What I have observed is, it seems everyone wants to take a System Administrator (SA), make him/her a Cyber SME or even an organization's cyber expert, and those two skills sets are not one and the same. I do not disagree that a SA has unique skills that can complement cyber security, but there needs to be more specific cybersecurity education/training/certification and a recognition by senior management that there is more to cyber than hacking and ensuring STIGs are applicably applied to a system.

•Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline?

Response: No, it isn't until recently that cyber has been seen as a necessary capability for sustaining a business. Lots of companies don't fully grasp that fact while they are attempting to build a cybersecurity-focused workforce. There is a huge skill gap between Senior Cyber expert and college students/recent graduates. Too many businesses are seeking to hire senior cyber personnel to do basic diagnostics, patching, etc., when those tasks can be done by more junior cyber-skilled people. Senior-level folks should be hired to oversee the design, implementation and sustainment of the best possible networks/systems, and that's what most companies don't get. I have also noticed that expectations are almost always more tactical versus strategic in nature.

•How do these types of knowledge and skills vary by role, industry, and sector, (*e.g.,* energy vs financial sectors**)?**

Response: Historically, DoD has been the largest entity to have embraced Cyber/IA. There are defined DoD mechanisms in place to optimize sound cybersecurity practices/designs. Financial, health and energy industries, however, are just beginning to take cybersecurity seriously. The more these sectors encounter cyber attacks, the more inclined they are to realize the need for cybersecurity, but they still tend to be reactive and tactical in their approach, versus proactive and strategic. They have a long way to go but they can certainly

learn from the DoD's long (and sometimes painful) history of implementing IA/cybersecurity.

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?

Response: To me, “Capture the Flag”has been a successful means to garner the enthusiasm and talent of our technology-capable youth in helping identify and protect our IT assets. There should be similar kinds of real-life examples and opportunities in other areas of cyber defense and offense career areas.

6. What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?

Response: Challenges are 1) fill the shortages in the senior and mid-range experienced personnel, 2) bring the financial, healthcare and energy industries to an acceptable level of cyber security, and 3) educate the general population on basic cybersecurity principles and practices. Regarding opportunities, I think the concept of IoT is new enough that we can get ahead of it, rather than always trying to play catch-up.

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)?

Response: For both questions, there is a need to educate and help guide private and public industries toward seeing cybersecurity as part of their business model similar to HR, Recruiting and IT. Too often, I see where cybersecurity is embedded as part of another organization. Senior cybersecurity personnel need to be at the table when it comes to making business and IT risk decisions and not be seen as an add-on, or even as unnecessary hindrance.

There is a lot of emphasis on educating the next generation; however, it is the Senior Executive level folks who make the budget and business decisions. They are the ones who need to understand and appreciate the fact that good cybersecurity will save money and heartache over the long run. Getting them up to speed is a bigger challenge than training entry level folks.

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? **Continued emphasis on identifying a centralized body to oversee cyber certification, education, and accreditation. Organizations want to**

protect their highest value assets from cyber threats, but there are so many different paths and providers, it's hard to decide which direction to go.

ii. At the state or local level, including school systems? **Continue to promote cyber education at an early stage, and to make it a priority for their local businesses.**

iii. By the private sector, including employers? **They should align themselves with governing federal guidance, policies AND ensure they implement the latest defense mechanisms to protect against cyber threats.**

iv. By education and training providers? **Continue to keep cyber classes timely and relevant, and require a basic cybersecurity course in most bachelor degree programs.**

v. By technology providers? **Continue to work with the community in identifying threats, educating users, and sustaining products that address cyber security. Additionally, address the issue of legacy equipment in the consumer's hands to avoid the next Wannacry, which affected more than just the consumer.**