Cybersecurity Workforce RFI

Pluralsight Response

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.

Pluralsight is a technology learning platform that empowers CIOs, CTOs and their teams to gain a competitive edge and succeed in the digital age. With adaptive skill tests, customized learning paths, 6,000+ expert-authored courses, interactive labs and live mentoring, Pluralsight helps enterprises learn and adopt the most critical technologies faster. Organizations around the world, including 40 percent of the Fortune 500, use Pluralsight to acquire the latest technologies skills and deliver the next big innovations.

Pluralsight has a dedicated information and cybersecurity content category. With the aim to close the global technology skills gap and help companies navigate digital transformation initiatives, Pluralsight provides cybersecurity professionals with high-quality learning resources, covering topics such as penetration testing, digital forensics, incident response, malware analysis, auditing, and secure coding practices.

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?

Currently, to the community's disadvantage, there is not one single source of truth that provides metrics and/or data related to cybersecurity education, training and workforce development program needs. Cyber Seek, www.cyberseek.org, provides a piece of this information in the form of cybersecurity credential holder counts, and if the information presented by Cyber Seek could be expanded to include data for cybersecurity education, training, and workforce development programs, it would provide a more holistic view of the present and future states of the cybersecurity workforce.

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

Currently in the market, there is insufficient understanding and agreement about workforce roles and the skills required for individuals to be successful in those roles. This need for alignment is becoming urgent, particularly with the rising need of qualified cybersecurity professionals. However, we do see a future where roles and required skills levels are openly communicated and understood throughout the industry.

One way we see this void being addressed is through the new version of the NICE Cybersecurity Workforce Framework, which will provide a lexicon upon which understanding and agreement around cybersecurity workforce categories, specialty areas, work roles, and knowledge/skills/abilities can be built. This--and other upcoming solutions--will address the discrepancies in work roles/titles that exist across the industry, especially given the new rise of roles that have emerged as a result of the fast-changing technology landscape.

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 most effective cybersecurity education, training and workforce development programs in the US today are programs that provide quality, timely instruction and guidance in a scalable, flexible format tailored to the individual learner. Historically, instructor-led training and technical bootcamps have been the industry norm for training technologists. These types of programs in today's fast-paced technology landscape, however, are often time-constrained, not scalable or flexible due to their in-person nature and limited in the ability to offer courses on the latest version of a given technology.

The 24/7 nature of SaaS-based technology learning platforms solves for the problem of scalability, removing physical constraints that limit the number of learners enrolled in the in-person, instructor led model. Technology learning platform Pluralsight provides its users with a flexible learning experience that allows its user to learn the latest and most relevant technologies. Through its platform, Pluralsight provides skill assessments that measure a person's given skill set and then provides them with a customized learning path that outlines the most direct path to increased proficiency in a given technology. Learning paths are comprised of courses created by industry experts and are continuously updated to ensure users are able to acquire the latest skills.

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

The shortage of skilled cybersecurity professionals is a challenge felt globally by employers trying to fill cybersecurity positions. According to the *(ISC)2 Global Information Security Workforce Study*, https://iamcybersafe.org/wp-content/uploads/2017/07/N-America-GISWS-Report.pdf, the industry is "…on pace to reach a cybersecurity workforce gap of 1.8 million by 2022."

Employers also struggle to retain the skilled cybersecurity professionals they already have. According to *The State of Cyber Security Professional Careers (Part I): An Annual Research Project (Part I)*, http://c.ymcdn.com/sites/www.issa.org/resource/resmgr/press_releases/ESG-ISSA-Executive-Summary-S.pdf, undertaken by ESG and ISSA, almost half of the respondents claim to be solicited by recruiters at least once per week. In this same study, 30 percent of respondents said their reason for being dissatisfied with their job is that their organization doesn’t provide ample opportunities for skills development. Employers are faced with the challenge of keeping their talent engaged in order to combat the onslaught of job offers with competitive salaries that their employees receive. For employers who wish to take an active interest in ensuring their cybersecurity professionals are engaged and fulfilled in their role, there are a number of options for fostering their employees’ growth. These range from creating a culture of learning so employees can upskill; supporting employee certification efforts; encouraging community engagements such as meet-ups, user groups, and conferences; and supporting participation in industry associations.

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)?

Rapid advances in technology are giving organizations across the world an ultimatum: adopt or become extinct. To remain competitive and minimize risk, leaders need provide their teams with an effective way to upskill on the most critical technology. To future-proof their organizations, leaders should monitor technological trends to inform their strategies and align team learning plans to meet real business objectives. Cybersecurity education, training and workforce development programs must support a culture of continuous learning and provide a way by which learners can acquire the latest technology skills quickly.