USCC™

US CYBER CHALLENGE

Cybersecurity Workforce RFI
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

August 1, 2017

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 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.

   Yes, the U.S. Cyber Challenge (USCC) directly identifies, recruits, and trains future members of the cybersecurity workforce while connecting them with potential employers. The USCC is an initiative of the non-profit Center for Internet Security, which focuses on safeguarding private and public organizations from cyber threats.

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?

NIST and federal agencies could better measure progress in training the cybersecurity workforce by implementing the recommendations laid out in the recent report "Increasing the Effectiveness of the Federal Role in Cybersecurity Education." The National Academy of Public Administration, Center for Internet Security, and Deloitte & Touche LLP published the report in 2015.[1] The recommendations to identify, track, and use performance indicators are:

a) "Collect information on graduates of CAE programs to enhance evaluation, improvement, and selection of graduates and schools

b) Develop and test to the "outcomes" features of Knowledge Units (KUs) and make results available (anonymously) to inform choice and encourage continuous improvement; consider competitions and challenges as hands-on testing environments; and

c) Test to scenarios or incident responses in addition to KU outcomes"

The federal government currently operates two, main cyber workforce training programs: NSA and DHS operate the National Centers for Academic Excellence (CAE) program and the National Science Foundation awards grants for the Scholarship for Service (SFS) program. Unfortunately, neither program collects data in a complete and consistent manner that would create a feedback loop to guide continuous improvement. Metrics to be collected include information from graduates about their educational experiences and information from employers about the skill levels of those employees they hire. In addition, the programs should make the data collected publicly available.

The report recommends schools that participate in the CAE and SFS programs should collect five types of data: time to securing a job; name and characteristics of first employer; additional training needed on the job; time spent on the initial job; and reasons for moving from job to job.

Moreover, Knowledge Units (KUs) make it possible for programs to evaluate how well students learned what they were taught and how well they can apply it. The Cybersecurity Enhancement Act of 2014 contains suggested KUs that can correspond to measures. These eight KUs are: (1) ethical hacking; (2) penetration testing; (3) vulnerability assessment; (4) continuity of system operations; (5) security in design; (6) cyber forensics; and (7) offensive and

[1] http://napawash.org/images/reports/2015/Cyber-CAE-Report-FINAL-10-15.pdf

defensive cyber operations, as well as (8) other skill sets determined to be appropriate in the future.

But organizations relying solely on KUs are likely to experience two main drawbacks: KUs test small parts of an overall process, but do not necessarily simulate the complexity of a real-world scenarios and KUs focus on technical skills but not critical thinking, decision making, and problem solving. Therefore, KUs should be mapped to the NICE Workforce Framework to minimize these shortcomings.

Additionally, government should focus on training programs that allow people with college degrees to receive incremental training to develop the necessary skills to obtain employment in a cybersecurity job today. These training programs should emphasize the fundamentals with an emphasis on good “hygiene” maintenance of systems.

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

   No, there is neither sufficient understanding nor consensus about workforce categories, specialty areas, work roles, and knowledge/skills/abilities. However, a DHS-sponsored taskforce created a framework for mission critical roles that can promote agreement in the cybersecurity workforce development community. In 2013, the Council on Cybersecurity released the report, “Job Competency Modeling for Critical Roles in Advanced Threat Response and Operational Security Testing,”[2] which describes these five mission critical roles. The report defines mission critical as, “work to be performed by the cyber functional role as being critical to the defense of an organization/agency’s information system.” The five roles are security monitoring and event analysis; incident responder in-depth; threat analyst/counterintelligence analyst; system and network penetration tester; and application penetration tester. The U.S. Cyber Challenge has used these roles to create a testing methodology (competition) against the roles and activities identified. The government can use this methodology as a roadmap to build out the remaining critical roles with national experts. More specifically, the method is a five-step process:

   1. “Establish vignettes (or scenarios) that define situated expertise in job roles
   2. Detail the goals and objective metrics that determine successful performance
   3. Identify the responsibilities by job role necessary to achieve the objectives

[2] http://docplayer.net/9857279-Mission-critical-role-project.html

4. Detail the tasks, methods, and tools along with how competence may differ in level of fundamental or differentiating indicators or expertise or the level of volatility, uncertainty, complexity, ambiguity that indicates the difficulty of achieving that level of expertise"
5. Develop the competition(s that will demonstrate the understanding of the roles

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, USCC operates following the appropriate cybersecurity policies because it is an initiative of the Center for Internet Security (CIS). The DHS National Protections and Programs Directorate provides funding to CIS; therefore, they are compliant with federal workforce education and training expectations.

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)?

   Current expectations of cybersecurity skills across government employers are neither necessarily aligned nor realistic. For instance, many federal organizations believe they should develop and operate their own Security Operations Centers, which includes hiring their own cybersecurity workforce. In reality, the primary role of most federal agencies is not security. Instead, federal agencies should leave the security mission to organizations that exist to provide it such as Microsoft, Google, and Amazon or a federal Line of Business in which an agency focuses on providing security to other organizations as a service. This specialization will reduce the need of every federal agency to build its own, separate cybersecurity workforce.

   In addition, public and private sector employers have a responsibility to encourage non-cybersecurity workforce employees to develop a cyber acumen. As the 2017 CSIS Cyber Policy Discussion Working Papers detail, "Acumen is defined as the ability to make good judgments and quick decisions, typically in a particular domain." This acumen includes a deep understanding of "how and where cyber is woven into the mission space of the organization or function."

   The federal government can implement a series of short, medium, and long-term recommendations to enhance the alignment between employers' needs and cybersecurity workforce skills, as detailed in the CSIS Cyber Policy Discussion Working Papers, published in early 2017.

Short-Term Recommendations

- Adopt Cyber Acumen as part of Senior Executive Service core qualifications
- Move the workforce practice within the DHS NPPD to the NIST organization where NICE initiative resides. This will align the statutory authority with the organizational responsibilities
- Devote the necessary resource levels to support cybersecurity education, training, and public awareness programs through the Department of Commerce and NICE initiatives
- Recruit one high-value cybersecurity candidate to federal service through a call from the President

Medium-Term Recommendations

- Adopt a system for accrediting training and education institutions offering programs in either theoretical or applied cyber science
- Adopt a taxonomy of cybersecurity roles and the specific skills that practitioners must demonstrate for competence in each specialty
- Adopt white-hat hacking courses including ethics at elementary and high school level supported by federal funding provided to states
- Develop specific veterans job recruiting program including an evaluation of existing programs to prevent duplication and expand the program that are working well

Long-Term Recommendations

- Develop a robust network of professionals and professional credentialing entities

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?

Both public and private entities are attempting to operate effective development programs for the cybersecurity workforce. Within the federal government, NSA and DHS National Centers of Academic Excellence and the National Science Foundation grants for Scholarship for Service programs are the two longest-tenured.

On an international level, the SANS Institute operates an online cybersecurity training program for up to 6,000 secondary school students in the UK. CyberStart offers an intensive training program, online game, and an advanced techniques program designed to help place the most talented participants in jobs. SANS is now making this program available to participants residing in six states in the U.S.: Virginia, Michigan, Hawaii, Nevada, Delaware, and Rhode Island. The U.S. program takes advantage of lessons learned from the UK and other global experience.

The common thread across the most effective public, private, domestic, or international cyber workforce training programs is hands-on, applied learning methods.

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

   Employers have a difficult time assessing the cybersecurity maturity of their organization and identifying the cyber skills they need when planning for an enhanced cyber workforce. Their needs include developing an understanding of their current and future desired capabilities to secure data and systems using their cybersecurity workforce. The Council on Cybersecurity (now merged into the Center for Internet Security) has proposed developing a Cyber Workforce Maturity Model (CWMM) to help organizations assess these needs. The CWMM would provide a consistent approach, common terminology, shared benchmarks, and the ability to collect data for measurement and continuous improvement. NIST can leverage this good work and continue the development of the CWMM to assist employers across the federal government and private sector.

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)?

All advances in technology -- including AI and IoT – will affect the future cybersecurity workforce. Policies, statutes, and treaties will govern the use of data and systems as emerging technologies are used by private and public sector entities. Workforce development programs must understand these emerging technologies, how they can be exploited, and then incorporate those new skills into their training and/or curriculum.

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?

   A Center for Strategic and International Studies report, "A Human Capital Crisis in Cybersecurity"[3] recommends several actions to grow and sustain the cybersecurity workforce. First, the Chief Information Officers Council (CIO Council) should adapt its biennial survey of the federal workforce focused on information technology to collect more detailed information about the cybersecurity skills of the workforce and identify any gaps. Second, DHS in conjunction with the CIO Council should establish a CyberCorps Alumni Group composed of the top 10 percent of graduates who complete the program. Members of the alumni group would receive training on CISO skills, networking, and leadership skills.
   Third, the federal government should use analysis from the Department of Defense (DoD) required by the National Defense Authorization Act of 2016 regarding the establishment of a "national guard" for cybersecurity type of approach.

   ii. At the state or local level, including school systems?

   The 2015 NAPA report recommends expanding the National Science Foundation's Scholarship for Service program to cover all public sector entities, including state, local, tribal, and educational entities. A "qualifying position" to pay off the Scholarship for Service funds now exist in federal, state, local, and tribal governments. Therefore, the program should be expanded to include the other levels of government.

[3] https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/101111_Evans_HumanCapital_Web.pdf

In addition, CSIS issued a discussion paper[4] on accelerating cybersecurity workforce development in early 2017 that advocates elementary and high school systems should establish required cybersecurity awareness training for all students to include online risks as well as general IT knowledge. CSIS also recommends federal funding be directed to support white-hat hacking curriculum, standard curriculum, and competitions to provide more opportunities for young people to develop awareness and knowledge of cybersecurity.

iii. By the private sector, including employers?

To produce accelerated results in the cybersecurity workforce, companies should advocate for an increase in the number of H1-B visas for skilled workers. The 2016 CSIS report "From Awareness to Action: A Cybersecurity Agenda for the 45th President"[5] recommends Congress create a new visa category for foreign cybersecurity workers who will work at U.S. companies that produce cybersecurity products.

iv. By education and training providers?

The 2015 NAPA report recommends expanding the Scholarship for Service program to include all two-year higher education institutions, regardless of whether they are formally associated with a four-year institution. The Cybersecurity Enhancement Act of 2014 authorized the program to provide support at community colleges. In response, the National Science Foundation extended the program to two-year schools that partner with a four-year institution so a student goes on to earn a bachelor's degree. However, not all students are a fit for a four-year education. Students who want to earn a two-year degree before entering the cybersecurity workforce should be supported also. Additionally, student participation should not be limited by their academic major but rather should take into account their desire to enter the cybersecurity field.

v. By technology providers?

Technology providers should raise their expectations of the skills graduating students have to keep driving higher standards and better training in the cybersecurity workforce development system. Many are currently investing in

[4] https://www.csis.org/programs/technology-policy-program/cybersecurity/csis-cyber-policy-task-force

[5] https://www.whitehouse.senate.gov/imo/media/doc/2016-01-03%20-%20CSIS%20Lewis%20Cyber%20Recommendations%20Next%20Administration.pdf

developing their own training programs but, in order to make this work, they should work jointly with the educational system so the students can participate in real life internship programs where they experience actual hands-on activities.