Response to RFI - Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development

Response by Haifeng Ji, Professor of Computer Science at Oklahoma City Community College.

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.

   I am a faculty member who teaches courses related to cybersecurity and information technology at Oklahoma City Community College. I am also the Point of Contact for Center for Cyber Defense Education (CCDE) at our institution. I am also the Cyber Club advisor at my college.

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?

   NICE Cybersecurity Workforce Framework is a great resource for cybersecurity training and workforce development. It is a national resource that categorizes and describes cybersecurity work. More awareness for this framework should be brought to colleges and universities.

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

   I believe there isn't sufficient understanding and agreement about workforce categories and work roles among many colleges and universities. However, more and more schools have started to adopt NICE Cybersecurity Workforce Framework. This framework would help schools to align cybersecurity curriculum towards workforce needs.

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

   N/A. As a computer science faculty member, I am not the spokesperson for the entire institution's security policy.

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)?

   Many employers require potential employees to have bachelor's degrees. I believe this expectation limits the number of candidates they can find. People with associate degrees who have sufficient experience/skills in the cybersecurity field should also be able to perform well in many job categories.

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?

   NICE Challenge Project and National Cyber League are two excellent programs. The NICE Challenge Project was created to test students on their ability to perform NICE Cybersecurity Workforce Framework tasks. National Cyber League provides a virtual training environment for participants to develop and validate their cybersecurity skills. These two programs are both effective and scalable.

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

   Many students who receive Associate Degree in Cybersecurity from community colleges do not have opportunities to transfer to area 4-year universities to get Bachelor's Degrees in Cybersecurity. I hope more 4-year universities are able to offer Bachelor's Degrees in Cybersecurity and offer transfer opportunities for community college students.

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)?

   Colleges and universities need to update their cybersecurity curriculums so that students can learn about the latest technologies and cyber threats. Schools with Center of Academic Excellence (CAE) designations are required to apply for re-designation every 5 years. The re-designation process

would ensure that cybersecurity curriculums are up-to-date in CAE designated schools. Oklahoma City Community College was recognized by the National Security Agency and Department of Homeland Security with the designation as a National Centers of Academic Excellence in Information Assurance 2-Year Education (CAE2Y) institution.

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?
   National Initiative for Cybersecurity Education (NICE) is a great program. It has helped many colleges and universities to improve their cybersecurity curriculums. It should be continued and expanded.

   ii. At the state or local level, including school systems?
   At the State level, efforts should be made so that more graduates from community colleges with cybersecurity degree would have the opportunity to transfer to area 4-year institutions to get their Bachelor's Degrees.

   iii. By the private sector, including employers?
   Employers should partner with colleges and universities to ensure that graduates would have the required job skills.

   iv. By education and training providers?
   More colleges and universities should incorporate NICE Challenge Project and National Cyber League in their curriculums.

   v. By technology providers?
   Cybersecurity technology providers should be encouraged to provide no-fee or low-fee academic software licenses to academic institutions for educational purpose.