Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development – Request for Information Response

Response by Energy Sector Security Consortium, Inc. (EnergySec) a United States 501(c)(3) non-profit corporation formed to support energy sector organizations with the security of their critical technology infrastructures.,

General Information

1. Are you involved in cybersecurity workforce education or training (e.g., curriculum-based programs)? If so, in what capacity?

EnergySec is a non-profit corporation that works in the energy sector. EnergySec works to identify the needs of the industry and to support colleges (both 2 year and 4 year institutions) as they educate and place students in the workplace. EnergySec also provides specialized training programs online, onsite, etc. for utility companies working through compliance and audit details associated with the NERC CIP standards.

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?

There are many programs that collect and analyze the data about cybersecurity programs and resources. What we find missing is a general “clearing house” of the information that is widely known to the industry and the HR departments within the organizations.

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

Although NICE has a workforce framework, it is not widely used in our industry to identify the security roles or job descriptions. The roles identified in the framework are mostly applicable to traditional Information Technology aspects of business vs. the Operational Technology (e.g. industrial control systems).

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)?

The Cybersecurity workforce is not well-defined as a profession. Many security professionals entered the field from related areas of specialty, such as networking; hence, there aren’t yet well-developed career pathways. Many energy employers are seeking workers who have a 4 year+ degree and 7-10 years of experience in what is a relatively new field. The workers that have those qualifications or the certifications based on those qualifications are very limited. Also, HR departments do not always have an adequate feel for what is required of cybersecurity workers or the job market so many times new prospects are not considered for

hire because they don't seem to have the right qualifications.

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 NSA CAE recognized 2-year and 4-year institutions are probably the best as they have a standardized set of learning objectives that can easily be used by employers to identify skill levels. Many other college programs offer only a few classes that can be directly related to cybersecurity and these classes are usually attached to another degree such as IT.
The NSA CAE programs are effective because they are strictly cybersecurity education.

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

A) Building the pipeline of workers, beginning in middle/high school. High school counselors need to have knowledge of cybersecurity as a career pathway with the options that this career provides students. Schools need to have access to cybersecurity speakers to excite students about the possibilities in a cybersecurity profession. Students need to have the opportunity to participate in high school programs like CyberPatriot competitions and 1NTERRUPT.
B) Standardizing the cybersecurity roles across industries so that the profession has definition for each stage of advancement, including educational requirements and time on the job that is realistic and matches the current shortfall of available workers.
C) HR training in cybersecurity skills needed to fulfill jobs that are available.
D) Entry-level jobs need to be developed to provide a bridge from the emerging academic programs to mid and senior levels positions.

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)?

Continued technological advancements will cause additional shortages in the workforce. New technologies may make security professionals more productive, but they will also add new risks and challenges that require human labor to address. Cybersecurity training and education programs must continue to adapt as the knowledge and skills required for proficiency in the security profession change rapidly. New models that are far more responsive to change than traditional post-secondary education must be deployed.

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?
Cybersecurity-specific apprenticeship programs should be developed to fill the current workforce gaps and provide a bridge from academic programs to careers in the security field.

What steps should be taken:
i. At the Federal level?

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

K-12 education must provide computer science courses to students.

iii. By the private sector, including employers?
Development of entry-level positions as well as internship and apprenticeship opportunities

iv. By education and training providers?

v. By technology providers?