EDMUND G. BROWN JR.
GOVERNOR

MARK S. GHILARDUCCI
DIRECTOR

Cal OES
GOVERNOR'S OFFICE OF EMERGENCY SERVICES

Strengthening the Cybersecurity of Federal Networks and Infrastructure: Workforce Development

Federal Register Docket ID: 170627596-7596-01

Comments from the California Governor's Office of Emergency Services

---

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?*

The California Cybersecurity Security Integration Center (Cal-CSIC) is working in direct coordination with Governor Brown's Cybersecurity Task Force (CTF) and our three core partners, the California Department of Technology (CDT), California Military Department (CMD), and the California Highway Patrol (CHP) to address the issue of creating and maintaining a well-trained cybersecurity workforce.

The CTF has identified the need to educate current and future cyber professionals and is addressing this issue through the Workforce and Education Development subcommittee. This subcommittee is charged with recommending the alignment and refinement of cybersecurity educational pathways. These pathways will include educational curricula, competitions, and professional development activities at the high school and university levels, with a particular focus on ensuring veterans and the underrepresented are included and are afforded opportunities in the field of cybersecurity.

To address the need to collect, organize, and share data pertaining to cybersecurity education, training, and workforce development, the Cal-CSIC is working through the Governor's Office, the Governments Operations Agency, and the State legislature. California distributed surveys to high school and college institutions to collect information about cybersecurity training and curricula. The Governor's Office recognizes the need to recommend and support the creation and funding of new and enhanced cybersecurity training programs in an effort to grow and maintain a high level of cybersecurity expertise.

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

Yes. California agrees that new cybersecurity categories and roles need to be created in order to maintain the cyber workforce necessary to protect the State from cyber criminals, bad actors, and hackers.

California, just like all state and federal organizations, is experiencing a lack of qualified cyber professionals to fill our workforce. Based on this need, the Cal-CSIC is working with CDT and the California Department of Human Resources (CalHR) to create new workforce categories, cyber-specific specialty areas, and position descriptions. The team created a specific list of knowledge, skills, and abilities (KSAs) that will be used to craft new cybersecurity job 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?*

On August 31, 2015, Governor Brown signed Executive Order (EO) B-34-15, which created the California Cybersecurity Integration Center. The EO charges the Cal-CSIC with creating a statewide cybersecurity strategy that is "intended to strengthen cyber emergency preparedness and response, standardize implementation of data protection measures, enhance digital forensics and cyber investigative capabilities, deepen expertise among California's workforce of cybersecurity professionals, and expand cybersecurity awareness and public education."

Workforce education and training are a top priority to Governor Brown, the Legislature, and the entire Cal-CSIC/CDT team. The policies created by the statewide cybersecurity strategy are the implementation steps California will use to enforce our workforce education and training efforts throughout the State.

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)?*

A strong cybersecurity workforce is dependent on effective analytic skills achievable through a "tiered" educational approach. The basic skillset employers desire in cybersecurity professionals are those attained through organizations such as CompTIA®, SANS®, and ISC2®. The basic knowledge required to enter into the cybersecurity workforce also depends on the specific area in which the respective employee will work (e.g. cyber threat analysis, forensics, etc.)

As responsibilities increase, so does the demand for a more in-depth understanding of cybersecurity principles. Employers expect a certain level of knowledge and expertise for their new hires to ensure they do not jeopardize their cybersecurity protective posture by appointing unqualified personnel into critical cybersecurity positions. These employers want to ensure the company security of personal, financial, business and operational information that is critical to the success of the organization. This expectation is realistic because of the ever-changing and increasing threats within the cybersecurity realm.

The students in the workforce pipeline currently do not possess the requisite knowledge and skills to fill the needs of employers throughout the nation. We need to continue to mature this process and support the creation of new and enhanced cybersecurity education and training.

The cybersecurity practice also dictates the need for various levels of industry-specific training (e.g. banking, health, critical infrastructure). In addition to cybersecurity principles, organizations must consider other regulatory guidance such as the National Institute of Standards and Technology (NIST), Federal Information Security Management Act of 2002 (FISMA), Health Insurance Portability and Accountability Act (HIPAA), North American Electric Reliability Corporation (NERC), Code of Federal Regulations (CFR) and Office of Management and Budget (OMB) regulations.

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?*

Determining the “most effective” cybersecurity program is greatly subject to interpretation based upon business industry. Organizations must consider a multi-tiered / multi-angled approach to cybersecurity to ensure all regulatory guidance is met. Companies must develop indigenous on-the-job training programs to complement formal training in order to ensure knowledge in transformed into the skillsets required to enhance their protective posture without hampering business processes.

Programs exist that are designed to provide the level of training based upon a tiered approach from entry level to advanced analytics and cybersecurity management. Organizations such as CompTIA® and SANS® have curriculum designed to meet entry level requirements. Other organizations such as ISC2® and SANS® have advanced programs to meet intermediate and advanced cybersecurity training requirements. The success of these programs is evident by the certificate and educational requirements requested in current cybersecurity job announcements.

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

One of the biggest challenges is that IT and cybersecurity need to be an integrated part of the overall business plan. There is a lack of common understanding of balance between an organization's need to have a strong cybersecurity program in place versus the success of their basic business model / financial bottom line. Many organizations still define IT support and cybersecurity as a "cost center." Calculations used to determine the company's Gross Margin do not include IT support and cybersecurity.

Another change is that cybersecurity training is costly and companies are still struggling to understand and report the cost of this training versus the benefit it will bring to the organization. Another major challenge is the recruiting efforts required to attract, hire and keep cybersecurity professionals with the required knowledge and skillsets. This requires employers to be willing to hire these professionals at typically higher salaries than they pay the rest of their business workforce.

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)?*

One of the biggest challenges facing our nation as it pertains to cybersecurity is for everyone to understand the balance between an organization's need to have a strong cybersecurity program in place versus the success of their basic business model / financial bottom line. Many organizations still define IT support and cybersecurity as a "cost center" and haven't changed their business model to understand that IT and cybersecurity are now an integrated part of the overall business plan. Calculations used to determine the company's Gross Margin do not include IT support and cybersecurity.

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:*

Federal and state governments should develop minimum standards for training, certifying, and assuring its cybersecurity workforce, similar to Department of Defense (DOD) 8570.01-M, Information Assurance Workforce Improvement Program. This standard requires agencies to assign levels to all IA (Cyber) workforce personnel in either Technical or Managerial positions. Each level (i.e. IA Technical Level III) requires certain minimum training and certification, experience, and security clearance requirements.

All government personnel should be required to be proficient and trained in basic cybersecurity principles and ethics upon initial hire, and annually thereafter.

i. At the Federal level?

Develop a standard program for cybersecurity personnel that include minimum training, certification, and personnel assurance (security clearance) requirements. Additionally, the government needs to provide additional funds for training, opportunities to exercise skills and sustain credentials (i.e. continuing education). Salaries should be commensurate with level of certification and experience rather than years of service.

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

Local and state governments should incorporate minimum standards that meet or exceed proposed federal standards for cybersecurity workforce training, certification, and personnel assurance requirements.

iii. By the private sector, including employers?

The private sector appears to be ahead of government requirements in cybersecurity workforce programs, perhaps because of their responsibility to shareholders and brand.

iv. By education and training providers?

Training and education providers must continuously assess and reassess the public and private sector cybersecurity needs and continuously improve their training programs to meet these needs.

v. By technology providers?

Providers currently offer training as a separate offering which can make it difficult for companies to grasp the total cost of ownership for certain cybersecurity software and hardware platforms. The cost of ownership is not defined correctly to cover the life of the product and the knowledge required to maintain and advance their protective posture. To assist in the advancement of cybersecurity, vendors should offer cost models that incorporate training and not add it as an additional line item that companies can choose to include or not.