Preparing Cybersecurity Professionals to Make an Impact Today and in the Future

On behalf of ISACA's community of more than 140,000 business technology and cybersecurity professionals, we would like to express our gratitude for the opportunity to comment on the Request for Information (RFI) seeking comments on growing and sustaining the nation's cybersecurity workforce.

By way of background on our organization, ISACA is a global business technology professional association that regularly leverages the expertise of our professional members in information security and cybersecurity, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology. ISACA has a presence in more than 188 countries and includes more than 215 chapters.

The following is an overview of ISACA's feedback:

1. Are you involved in cybersecurity workforce education or training (*e.g.,* curriculum-based programs)?
    a. Yes, ISACA staff and some members are heavily involved with cybersecurity workforce training. Specifically, ISACA has a cybersecurity team in charge of oversight of our Cybersecurity Nexus (CSX) Program, which primarily focuses on workforce development via technical, skills-based training. Through ISACA's CSX Performance-based Training Platform, we can train security professionals and those who aspire to be security professionals in cloud-based, live environments. Training participants are taught real skills through training and lab work that is aligned with both the NIST workforce development framework as well as the NIST Cybersecurity Framework (NIST CSF). Cybersecurity professionals can also pursue the CSX Practitioner (CSXP) certification, the first-ever vendor-neutral, performance-based certification for cybersecurity professionals. The hands-on platform offers step-by-step scoring and assessment with direct feedback on individual strengths and weaknesses so students can easily identify and address areas they need to address.
    b. Additionally, the organization offers a variety of educational tools to support cybersecurity audits. These include, but are not limited to, the following:
        - **Implementing the NIST CSF** –https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Implementing-the-NIST-Cybersecurity-Framework.aspx
        - **Audit program – Cybersecurity: Based on the NIST Cybersecurity Framework -** http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-Based-on-the-NIST-Cybersecurity-Framework.aspx

- **White Paper – Auditing Cyber Security: Evaluating Risk and Auditing Controls -** http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/auditing-cyber-security.aspx
- **Webinar – Suggested Tips Auditors Need to Know About Cyber Security -** http://www.isaca.org/Education/Online-Learning/Pages/Webinar-Suggested-Tips-Auditors-Need-to-Know-about-Cyber-Security.aspx
- **Webinar – Tips for Auditing Cyber Security -** http://www.isaca.org/Education/Online-Learning/Pages/Webinar-Tips-for-Auditing-security.aspx

c. At ISACA, we are fortunate to have dedicated and engaged volunteers. One example is a volunteer who has taught training courses, including ISACA CSX, ISACA CISM, participated in the C-CISO training exam, co-wrote the C-CISO Body of Knowledge, participated in CSX development, wrote a chapter for the (ISC)^2 Official CISSP Study Guide, contributed to COBIT 5 for Information Security, wrote books, at least one of which is used in several university cybersecurity programs (Information Security Governance Simplified: From the Boardroom to the Keyboard), and presented at ISACA conferences.

Growing and Sustaining the Nation's Cybersecurity Workforce

1. What current metrics and data exist for cybersecurity education, training, and workforce development, and what improvements are needed in the collection, organization, and sharing of information about cybersecurity education, training, and workforce development programs?
   a. Current data comes from academic institutions, particularly the National Centers of Academic Excellence (CAE). However, we are less aware of progression from community colleges, traditional university and college programs, and global concerns. In the professional arena, we can determine from reported data that there remains a significant skills gap, and that the job demand is outpacing the number of qualified candidates. Global workforce studies such as the (ISC)^2/ Frost and Sullivan study as well as ISACA's State of Cybersecurity give us input but do not provide us with the reasoning. There is still a need to be surveying high school students to determine if they are interested in pursuing a career in cybersecurity or an associated program, and if not, why? How can we make these careers more attractive to young people? The scholarships for service are a nice way to eliminate debt and guarantee a job. Are there opportunities to move these types of programs into community colleges or vocational schools so that we can reach a broader audience who may not be interested in

theoretical-based management programs but instead display aptitude for technical analysis and architecture roles?

b. Dissemination of the data is adequate. Organizations are routinely reporting about information/cybersecurity, and government technical media disseminates the reports. Regardless of whether the data are rooted from a nonprofit professional association, a vendor such as CISCO, a professional services firm such as PWC, or a government agency, the data are available. However, it is harder to determine what is an "official" or endorsed workforce development training program. The training provider landscape is very large – higher education institutions, contractors for DOD, nonprofit associations, for-profit training partners; it is hard to tell if there are paths that are more beneficial than others.

c. There is a lack of awareness by industry of a good measure of how many security professionals exist, years of experience, and how many are 'in the pipeline' at colleges and universities. It is also very important to stratify the demand by job type – are these CISOs that are needed? Cybersecurity analysts? Forensic practitioners? They all get lumped into "one statistic of 1.8 million jobs short by…"

d. One approach is to implement information sharing across organizations and industries on training and education practices and course work that have shown success so that we can democratize the knowledge and raise the overall bar of the workforce's skills in cybersecurity areas.

e. Most cybersecurity training today is knowledge based versus performance based. With cybersecurity, it is critical to teach hands on skills.

f. Also, there isn't enough focus on good security practices, secure coding and development life cycle, and OPSEC and InfoSec practices in pre-university and university course work. Cybersecurity needs to be reinforced in the workplace through testing and scenario exercises so that the knowledge can be applied to practical examples and events.

g. Trainees are also lacking career paths to follow when seeking further instructional courses. For example, what type of training should someone who wants to be in incident response follow? Forensics? Cybersecurity management? This type of clear guidance would help individuals to set clear paths and get to work with the right skills faster.

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

   a. The categories in 181 are easily understood and much improved since the last release where there seemed to be a large gap in the vernacular used in it versus that of industry.

b. The 'profession' as we know it today is less than 25 years old. The cybersecurity arena continues to grow in complexity and taxonomies and focus areas continue to evolve. There needs to be a balance between core skills and specialty expertise and training. For example, network and platform security is a necessary core skill but is often challenged when applying those tactics to evolving architectures like IoT.

3. Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?
    a. ISACA has established cybersecurity policies that have been developed to fit the needs of the organization, a non-profit membership association. With that, the policies are based on a few industry standards of information security controls such as ISO 27001, NIST SP 800-53 and COBIT® 5. At the present time, there is not one specific standard to directly compare against.

4. What types of knowledge or skills do employers need or value as they build their cybersecurity workforce?
    a. This answer depends on the type of role for which they are hiring. If an enterprise is looking for a CISO they need to be looking for a strategic leader who has experience communicating with executives and with technical teams. This person needs to understand that the security objectives must support and align with overall enterprise objectives. Risk management, governance, business skills and people skills are all critical in this space. This person does not need to be a technical expert but does need a solid understanding of the threat landscape, controls to address threats, how to work strategically with third parties, and efficient ways to address regulation and compliance requirements.

       If the employer is looking for a SOC analyst, the focus needs to be on technical analysis skills rather than risk management issues. Candidates need to understand packets, scripts, tools and technologies used to control/countermeasure threats and attacks. They need to be skilled at log monitoring and hunting for attacks. They need to have strong incident response skills. They need a strong sense of urgency.
    b. Additionally, employers need to support continued education and training to both reinforce core security skills and practices as well as provide the specialty and niche trainings and education for the evolving use cases, technologies and architectures to stay in front of the cyber challenge curve.
    c. Most employers are looking for something beyond 'book knowledge' and want to know that candidates have some practical experience. This is difficult; as one volunteer reports, "In my organization, we are starting a new college graduate 2-year rotational development program, and I am leading it. We need to partner, as organizations, with

colleges and get the right skills in place, but also companies need to nurture this." He adds, "The problem comes in for smaller companies, that can only afford 1-2 people in their 'headcount' – so they want experienced people because they don't have anyone to train them. The positions then remain open as they want to pay a junior salary to an experienced person. If they do find someone, they end up leaving for a company that will pay market rate."

5. 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. Frequently, employers and human resource recruiters do not understand what they are looking for and so they create job descriptions that attract "unqualified" candidates. Employers cannot expect a new-to-the-profession technician to be an expert in ISO, CSF, COBIT, or other governance and management frameworks. They cannot expect technical analysts or pen testers to understand risk management. Likewise, it is unreasonable to expect a CISO or security director to be configuring firewalls or creating python scripts. It is very important that we create the right guidance regarding skills, training, experience, certifications, etc., so that enterprises can bring in the right level of professional to ensure that the security programs are staffed in the best way possible.
    b. There are some key differences across industries, but they are not skill based. However, a security manager in the financial services industry is going to need to understand the financial services regulations; whereas, someone in healthcare will need to understand the specific requirements that the industry regulation imposes. Energy might be a bit different because the sensor systems involved in SCADA frequently need additional skills that are not inherent to a typical network.

6. 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?
    a. This is very difficult to assess. There is no scale of which we are aware that currently measures whether employee contribution is tied to overall better security within an enterprise and then mapped back to a training program.
        i. The fundamentals of security, networking, business, governance and risk are all being taught. The problem is that each of these is its own discipline. As a result, students are getting more of a "jack of all trades" education than a deep dive into

each specialty. Their training is also most often based in theory. They receive very little hands-on training; thus, the skill sets need to be developed on the job. If people do not supplement their training and education with on-the-job experience, an apprenticeship or an internship, they will not be prepared to face the challenges that enterprises are encountering. ISACA is supportive of the scholarship for service because of the opportunity to provide practical, hands-on experience.

ii. These performance trainings can be delivered at conferences and training events, in the academic environment and within organizations as part of their ongoing training and workforce education. Additionally, cross-division, organization and industry information sharing on education and training content will help prepare the workforce for emerging and new challenges as well as help reduce skill gaps that may become evident when organizations will typically focus on a limited area of cybersecurity relevant to their current environment.

b. Specific training recommendations include: ISACA CSX, CISSP by $(ISC)^2$, SANS technical courses, EC Council's Certified Ethical Hacker course and CISM. The IAPP Privacy training should not be excluded either if we expand the notion of cybersecurity into information security. ISACA believes the industry still recognizes these more than university programs.

7. What are the greatest challenges and opportunities facing the Nation, employers and workers in terms of cybersecurity education, training and workforce development?
    a. There are not adequate numbers of students entering the field. This especially holds true with females and minorities. The military has a very strong approach to training its personnel, and this may be an opportunity to leverage talent that already exists. If technical cybersecurity programs were offered as vocational careers, we would have a much bigger candidate pool. Right now, cybersecurity degrees are most common in higher education systems, but many people cannot afford to attend these types of programs. By making the programs affordable, the US will be able to train many more people in the deep technical skills needed to identify, protect, detect, respond and recover from cybersecurity incidents.
    b. Making cybersecurity attractive to people as a lifelong career is important. We are also missing a huge opportunity and are not marketing to women correctly, as only 11% of the talent pool are women. This should be closer to 50% if women are appealed to in the right way.

8. How will advances in technology (e.g., artificial intelligence, Internet of Things, etc.) or other factors affect cybersecurity workforce needs 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)?
    a. The programs need to be training people on up-to-date technology, threats and tools. For the most part, the foundations do not move too much but the technology and the threat landscape do change and evolve.
    b. Emerging technologies and architectures will drive the need for cybersecurity workforces to understand and be fluent in these innovations. For example, understanding the complexity of IoT deployments, comms/protocols and platform building blocks requires new skills and experience not typically gained in standard IT environments, so IT Sec and OT Sec need to come together to best assess risk and implement security controls and mitigations jointly. Another example may require ITSec, OPSEC and InfoSec teams to partner with data scientists and analysts to manage and implement the proper security controls for machine learning and AI, and operationalize them while supporting the business goals and objectives.
    c. Additionally, these new technologies and architectures can augment and enhance cybersecurity capabilities, whether through IoT style security sensors or the use of analytics and AI, to more efficiently and accurately detect emerging and unknown threats, as well as use of AI and machine learning to better automate response and mitigations to security events.
    d. Most companies may ‘talk’ about these things, but few are making serious investments in them yet. This is the current industry hype with vendors selling products. We need cybersecurity people who fundamentally protect organizations; most will not be dealing with these concepts in earnest for 5-10 years.
9. 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?
        - An increase in funding and focus for academic programs on cybersecurity practice and skills.
        - Improved and broadened industry – government talent sharing (Employee/Worker Exchange programs). Funding and creating programs where the cybersecurity workforce from industry and government can more naturally and easily take posts outside their organization for periods of time to expand their skills, mentor the local talent, and share best practices and experience.

- Just like laws mandated the need for CISOs, ensure that a workforce training program is in place for the public and private sector, mandating at least 40 hours training per year per cybersecurity employee.

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

- Vocationalism for cybersecurity roles
- Similarly, state and local government can fund education programs and institute talent exchange cybersecurity programs as well as host security hackathons and scenario-based war games.
- Have a standardized register of titles and training at the school level that matches NICE, with a rating system so we can see what is out there.

iii. By the private sector, including employers?

- Employers can improve their cybersecurity workforce by participating in talent exchange programs, funding continued education and training for their workforce and proactively encourage cross-division, organization and industry content sharing, as well as cross-division, organization and industry security hackathons and scenario-based war games (including hands-on training).

iv. By education and training providers?

- Increase frequency of updates on training courses. Include skills-based training.
- Education and training providers can improve the cybersecurity workforce by hosting cross-organization and cross-industry security hackathons and scenario-based war games. They can also provide course work and classes that marry content on security practices, secure coding and development life cycle, and OPSEC and InfoSec practices in hands-on lab environments applied to real-word scenarios and case studies.

v. By technology providers?

- Continue to produce training with content and technology updates.
- Technology providers can augment continued education with sponsored training and integration with external organizations and partners to provide more real-world hands-on skills for the cybersecurity workforce. They also should focus on the user experience and ease of use, deployment, integration and operation of their products and technologies to help ease the specialization requirements for the workforce that will have to manage these environments.