(ISC)² Response to NIST RFI – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development

On behalf of (ISC)²® and its 125,000 plus members, we are pleased to provide our response to the NIST request for information – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development. (ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, programmatic approach to security.

As the cyber threat continues to evolve and expand, it is critical that the U.S. public and private sectors have a trained workforce in place to meet the challenge of securing our interactions in cyber space. Advances such as the Internet of Things, and Artificial Intelligence will bring hundreds of millions of new devices online in the next few years. This will further stretch our already thin cyber workforce. We face a significant shortage of cyber professionals, and the gap is widening. The current approach is not meeting the needs of the public and private sectors. We need renewed focus and investment to close the gap and better protect our cyber infrastructure.

The 2017 Global Information Security Workforce Study (GISWS) recently released by the Center for Cyber Safety and Education and sponsored by (ISC)² shows that we are on track to reach a cybersecurity workforce gap of 1.8 million by 2022. This represents a 20% increase over the 2015 study and a step in the wrong direction. The 2017 study included responses from over 19,000 cybersecurity professionals from 170 countries, including 2,620 professionals that work on federal systems, including both federal DoD and federal civilian employees and contractors. Threats continue to rise and diversify. According to federal respondents (87%), hiring and retaining qualified information security professionals remains the number one factor in effectively securing an organization's infrastructure. Further, the shortage of information security workers continues to take a toll on the federal government's ability to operate effectively and efficiently, with respondents saying that the scarcity of talent negatively affects the existing information security workforce (79%), the organization as a whole (68%), customers (63%) and security breaches (49%). The problem is getting worse.

We applaud the federal government's recognition of this critical challenge and support the National Initiative for Cyber Education's (NICE) work to try and close the gap. Clearly, more needs to be done and a broad public private partnership is necessary if we are to make progress to close the cyber workforce gap and help better secure our national cyber infrastructure.

We have provided our responses to the questions posed in the RFI below. We have also included the 2017 GISWS as supplemental information. (ISC)² and its members look forward to working with the Department of Commerce to find workable solutions to the current cybersecurity workforce challenge.

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?**

Historically, certification bodies like (ISC)² led the way by establishing education, experiential and certification metrics to provide hiring officials assurances that the people holding one of our certifications have both experience and demonstrated knowledge, skill and ability to perform in cyber, information, software and infrastructure security roles. Certification bodies like (ISC)² that are accredited by ANSI against an international standard like ISO/IEC 17024 on an annual basis have established rigor in their process of ensuring the integrity of the certification process.

Academia has made progress, but these programs vary considerably. Lack of standards still hinder the ability to gauge the student's ability to perform in the workplace upon graduation and formal education does not always come with experience. Additionally, the term certificate and certification are often used synonymously, when they are not synonymous terms. The Institute for Credentialing Excellence provides an excellent comparison between certificate and certification:

Assessment-based Certificate Program	Professional or Personnel Certification Program
Provides instruction and training (non-degree granting)	Assesses knowledge, skills, and/or competencies previously acquired
Goal is for participants to acquire specific knowledge, skills, and/or competencies	Goal is to validate the participant's competency through a conformity assessment system
Assessment is used to evaluate mastery of the intended learning outcomes; linked directly to the learning event	Assessment is best used to assure baseline competencies and to differentiate professionals; independent of a specific learning event
Assessment content may be narrower in scope	Assessment content is usually broad in scope
Awards a certificate to recognize mastery of the specific learning outcomes; it is NOT a certificate of attendance or participation, which is awarded to individuals who have attended or participated in a course or training program but did not have to demonstrate mastery of the intended learning outcomes	Awards designations to recognize achievement
To earn accreditation, complies with the *ICE 1100 Standard* and follows the ACAP application procedures	To earn accreditation, complies with the *NCCA Standards for the Accreditation of Certification Programs* and follows the NCCA application procedures

At (ISC)², we're proud of how the international cybersecurity marketplace has responded to the work we've put into our certifications and the assurances provided by candidates and employees who hold one of our certifications.

With regards to metrics, there's still considerable consumer confusion and debate within the industry when statements like "hands-on" examination is superior to traditional closed-end stemmed items when it comes to assessing knowledge. We can often look at how other organizations responsible for

important professional assessments operate. For example, the National Board of Medical Examiners has been assessing candidates for over 30 years and less than 5% of their examination is hands-on, whereby 95% of the assessment is in fixed format type items – multiple choice items with a known problem (i.e., the stem) and a list of suggested solutions known as alternatives with one correct or best alternative (i.e., the answer) and the incorrect or inferior alternatives (i.e. the distractors). Few will argue that hands-on when done correctly can provide great training, but perhaps hands-on is not always the best method for assessing knowledge.

"The State of Cybersecurity from the Federal Chief Information Security Officer's Perspective"—An (ISC)² Report was the industry's first comprehensive survey of Federal Chief Information Security Officers (CISOs) in 2009 that identified critical challenges and trends developing in the federal cybersecurity workforce. Similarly, in 2010 and again in March 2016, (ISC)² surveyed a targeted pool of executive-level government officials and contractors from civilian, military and intelligence agencies to determine the state of cybersecurity and to provide recommendations for advancing the federal government's cybersecurity progress.

During alternating years, (ISC)² publishes the U.S. federal government results of the GISWS representing the opinions of both federal executives and practitioners regarding certification, training and education requirements for organizations and professional development; trends and issues related to information security; potential gaps in organizational security; and a forecast of what skills and positions will be needed most in the U.S. federal government over the next three to five years.

Moving forward, (ISC)² and its sponsors remain committed to surveying these important demographics of both cybersecurity workforce decision-makers and practitioners on a bi-annual basis in order to better understand the unique challenges and trends facing those responsible for nurturing the federal workforce. Report findings can be downloaded here: www.IAmCyberSafe.org/GISWS

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

NIST Special Publication 800-181[i] titled, "NICE Cybersecurity Workforce Framework (NCWF)," provides a fundamental reference resource for describing and sharing information about cybersecurity work roles, the discrete tasks performed by staff within those roles, and the knowledge, skills and abilities (KSAs) needed to complete the tasks successfully." Once finalized, this Framework should provide an excellent resource for workforce development, planning, training and education.

That being said, there is an understanding, that cybersecurity continues to evolve as new technological advancements occur, thus roles will also change.

It is also critical to distinguish between, and address the needs of, both the cyber workforce and the general workforce.

Regarding the cybersecurity workforce, the emergence of the Internet of Things and Artificial Intelligence as an example, as well as the Administration's push toward shared service/cloud environments will require new skills and knowledge. Likewise, technologies around platforms like industrial control systems and mobile will further require specialization. We believe that private industry working with government agencies like NIST can help define evolving workforce categories, specialty

areas, work roles and skill needs. In addition to government, a working group should be formed to tackle this issue and include representation from enterprises, practitioners, cyber education organizations and certification bodies.

Looking beyond the cybersecurity workforce to the broader federal workforce, we believe a greater understanding is necessary when it comes to requisite knowledge/skills/abilities and training. "People," through actions both intentional and neglectful, remain the greatest security vulnerability to federal agencies. Therefore, advancing an organization's security agenda no longer rests upon educating its cyber workforce, rather it must educate its entire workforce, across all departments, in cyber. From the intern to the CEO, the mindset needs to be, "Cybersecurity is everyone's job." To achieve this, we need to encourage cybersecurity cross-training to promote cyber literacy across all departments within federal agencies. Agencies must have training dollars set aside to train non-cyber employees. Non-cybersecurity personnel are essential in helping to win this battle. An educated general workforce will help offset the shortfall of cyber workers.

We do not believe there is strong agreement when it comes to workforce categories, specialty areas, work roles and knowledge/skills/abilities. (ISC)² has been an international leader in this area through our Common Body of Knowledge (CBK) that establishes a common lexicon for our 125,000 members around the world. Our Certified Information Systems Security Professional (CISSP) certification is the most widely respected cybersecurity certification around the world. Many private and public sector organizations require the CISSP for positions of trust related to cyber, information, software and infrastructure security.

However, the cybersecurity industry seems poised to continue to add the growing number of job types within the industry, which further confuses career candidates, applicants, hiring officials and public and private sector leaders. We believe this is one reason that our CISSP certification has been so successful. Hiring officials understand that a CISSP understands the programmatic nature of cybersecurity regardless of varying job titles and areas of responsibility. The CISSP understands that a holistic approach is paramount to designing, implementing and maintaining a meaningful cybersecurity program.

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

As a cybersecurity certification body, (ISC)² does have appropriate cybersecurity policies in place regarding our workforce education and training efforts. These policies are regularly and consistently enforced. We educate professionals on how to establish the necessary cybersecurity program, which is a far broader requirement than deep technical skills. Programmatic and deep technical skills are required.

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)?

At times, there are unrealistic expectations within the industry. For example, to hold an (ISC)² CISSP certification requires five years of experience, yet we'll see entry-level positions advertised as requiring a CISSP. CISSP holders command anywhere from 25% to 35% more than those who do not hold the

certification. It's unlikely that a CISSP would be interested in an entry-level position. Conversely, the Associate of (ISC)² program is perfect for entry-level candidates. It demonstrates that the individual has passed a rigorous examination process, has met annual continuing professional education (CPE) requirements and only needs the experience to qualify for the (ISC)² certification related to the examination they passed. Based on (ISC)²'s Center for Cyber Safety and Education's research, expectations across all industry types are not being met when it comes to having enough qualified cybersecurity professionals.

There are various aspects of cybersecurity knowledge and skill that are consistent and transcend role type and industry type. There are also specialty areas like industry control systems, healthcare, finance and cloud security that have unique considerations that the workforce needs to be prepared for.

The 2017 GISWS (attached) provides a road map of what the emerging threat areas are, what skills are needed and where there are gaps in today's workforce. Specific to the federal government, the greatest training and education needs within IT over the next three years will be:

- Cloud computing (61%)
- Information risk management (44%)
- Incident response (44%)
- Security engineering (43%)
- Threat intelligence (42%)

Yet, there appears to be a discrepancy regarding what skills are most important for cybersecurity professionals to acquire. Information security professionals think they should focus most on acquiring cloud computing and risk assessment and management capabilities, while hiring organizations look first for candidates with strong communication and analytical skills.

Overall, employers' expectations are realistic provided we can continue to focus on increasing capacity to grow the workforce, and can provide sufficient training and certification to ensure that workers have the knowledge and ability to do their job well.

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?

In today's world, a sense of mission doesn't always override good pay – incentives work. For example, following the cybersecurity hiring authorities passed by Congress in 2014, the Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) provided pay incentives at 20-25% above an employee's annual pay to motivate new cybersecurity hires. The practice of incentive pay needs to be replicated throughout the federal government in order to attract experts from the private sector. This perk also plays a key role in retaining cybersecurity talent. According to the Pew Research Center[ii], millennials recently surpassed Generation X as the largest generation in the U.S. workforce.

The 2017 (ISC)² Global Information Security Workforce Study found that paying for professional memberships and training are key drivers in job satisfaction with this demographic.

That being said, in our best effort to attract and retain top cyber talent, we are handicapped by the government's antiquated general schedule (GS) classification and pay system that makes it difficult to promote high-achievers and re-position non-achievers. One such reform effort should be further considered – the "cyber national guard" concept – which would allow the federal government to repay student loans of STEM graduates who agree to work for a number of years in a federal agency before returning to the private sector. This will serve as a natural extension to the existing Scholarship for Service (SFS) program and will help to expand the broader workforce development initiative.

The "Cyber Corp" model is another example of an effective workforce program. Modeled after the existing US-CERT program, agencies should be able to loan/borrow cybersecurity personnel resources in times of need. This could be accomplished through the establishment of a Federal Cyber Corps against which all agencies could draw without local Human Resources involvement.

Overall, the most effective cybersecurity education and training workforce programs are those developed by cybersecurity professionals who can apply their practical knowledge in partnership with academia and training organizations. We need a continuous education cycle that starts in elementary school to raise awareness, expands in high school and college to apply practical knowledge and is regularly updated for the cybersecurity worker to meet the changing cyber threat landscape. The goals of these organizations should be two-fold: to close the current workforce gap and to ensure that current cybersecurity professionals have the knowledge and skills to protect against evolving cyber threats. One example includes The Center for Cyber Safety and Education's Safe and Secure Online program that brings certified cybersecurity experts – (ISC)² members – into classrooms across the world to teach children how to protect themselves online and become responsible digital citizens.

The CISSP program is the most successful cybersecurity certification program in the United States and around the world today. (ISC)² has roughly 82,000 members in the United States, and 94% of them members hold the CISSP certification. We have over 20,000 members in the National Capital Region. (ISC)² is a nonprofit organization whose vision is: "To inspire a safe and secure cyber world."

The CISSP credential provides an international standard for private and public-sector organizations regarding cybersecurity.

Finally, the cybersecurity resource lifecycle maturity model must evolve to include the assumption of rapid cybersecurity personnel turnover and modify the approach in order to establish a network of resources to backfill positions. The assumption of turnover must also be incorporated in the agency's training program.

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

Foremost, our research indicates that the cybersecurity workforce is aging, and we're simply not reaching new profession entrants like millennials and career change candidates. The volume, sources and complexities of attacks continue to mount as our existing workforce is stretched thinner and thinner. One of our major challenges is attracting people to the cybersecurity profession. We also lack diversity within the current cybersecurity workforce. Globally, women make up only 11% of the cybersecurity

workforce. We know within the United States, other minority groups are also underrepresented within the current cybersecurity workforce. (ISC)²'s Center for Cyber Safety and Education will release its first diversity report in September of 2017 in hopes of raising awareness about the need to draw from all pools of talent. The millennials are the largest and most diverse generation of our time. We need to find ways to attract millennials into cybersecurity. This can start in secondary schools, and (ISC)² has worked hard to adapt some of its content for secondary school use. However, secondary schools often lack teachers who are qualified to present cybersecurity topics.

The current shortage of cybersecurity professionals creates a significant risk to our economic and national security. It is a risk that must be mitigated. It will take the cooperative effort of the federal government, academia, private sector and organizations like (ISC)² to help close the gap. In order to accomplish this, we must:

- Increase capacity at community colleges and universities to help meet the demand. These universities should partner with training and certification organizations so that students can be prepared to hit the ground running as soon as they graduate from a two-year or four-year institution.
- Invest in and focus on expanding training and certification programs which will be essential to ensuring that individuals are prepared to protect against the cyber threat. Likewise, the private sector must invest in growing the workforce, increasing capacity at universities and providing practical training opportunities.
- Dedicate resources to regular and continuous cyber hygiene training and simulation drills, cyber range activities and practical exercises that engage users at every level.
- Dedicate resources to retaining existing cyber talent. Given the multiple factors working against the government's efforts to build a skilled workforce, existing cyber professionals must be nurtured and rewarded with training and continuing education opportunities.
- Establish hiring standards that allow for limited changes by local Human Resources organizations.

Finally, we believe that efforts need to be made to attract more women and minorities into the field of cybersecurity. The current cyber workforce is predominately white males. In competing with the private sector for skilled professionals, hiring women and those from underrepresented groups should be a key component of the government's talent acquisition strategy given that, according to the 2017 GISWS, 70 percent of federal respondents say their organization offers a program that encourages diverse hiring in information security, compared to just 55 percent in the private sector. Diversifying the workforce will help close the current shortfall of federal workers, create a more heterogeneous environment and bring additional views around how best to combat cyber threats.

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)?**

Few if any professions stand still, and cybersecurity is no exception. The cybersecurity workforce will continue to evolve and change to try to keep pace. However, threat actors continue to employ both old and new vulnerabilities, so we need to continue educating on old attack methods while we advance the workforce regarding new attack vectors and methodologies. The Internet of Things (IoT) and the embedded nature of IoT will continue to expand the attack surface the cyber workforce will need to

assess and protect. These physical systems increasingly have embedded firmware and software that needs to be considered and appropriately protected.

We must prepare the current and future workforce to defend against these threats. The cyber workforce should have the intellectual and practical knowledge to do their jobs today and in the future. Therefore, cyber training and education must be ongoing, dynamic and accessible. Certification programs and continuing education need to be available and updated on a regular basis. The public and private sector must invest in their employees and offer opportunities for cyber education and training programs and further, employees should receive the financial support and the time off to participate in training and certification programs.

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?

The federal government should look at ways to speed up its hiring and clearance process when it comes to cybersecurity professionals. In addition, the government should support more training and certification programs for its existing cyber workforce, including expanding opportunities for training and providing financial support for certification programs. The federal government's cabinet agencies should consider adopting a DoD 8570 and DoD 8140 compliance approach.

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

Education systems at the elementary and high school levels need to integrate cyber programs into their curriculum to raise interest and awareness of cyber and cyber careers. Further, we need to train teachers with the skills to educate students and thus expand capacity at schools and ultimately grow the talent pipeline. At the community college and university level, we should be providing practical experiences through internship and mentorship opportunities and integrate certification programs so that employers can feel comfortable that graduating students are prepared with the skills and abilities to hit the ground running.

To avoid wasting time and resources, state and local levels – including school systems – should consider the approaches and framework taken on by the federal government and the DoD. Time is better spent on operationalizing an established approach or framework versus the "developed our own" approach.

iii. By the private sector, including employers?

The private sector should support continuing education programs for their workforce. Current cybersecurity professionals should have the opportunity to expand their knowledge base and gain the skills to combat emerging threats. Employers should also support internships and mentoring to help new potential workers.

iv. By education and training providers?

Education and training providers need to build scalable, adaptable programs that can meet both the growing demand for cyber education and training and can teach new skills when emerging technologies provide new risks.

v. By technology providers?

Technology providers should focus on more secure development practices, including software assurance. Risk will continue to rise as new threat vectors emerge. Billions of new devices as part of IoT will come online, often developed without security designed in. We need to change that paradigm and focus on building more secure systems and products.

Software and hardware developers need to do a better job of building security into their products and services early in the lifecycle of the product and throughout its lifecycle.

Technology providers need to continue to consider their responsibility to offer training on their technological solutions and services. In most cases, the developer or manufacturer of the product is best positioned to provide detailed and deep-dive training on their products.

---

[i] Draft NIST Special Publication 800-181: *NICE Cybersecurity Workforce Framework (NCWF) National Initiative for Cybersecurity Education (NICE),* Bill Newhouse, et al. November 2016, http://csrc.nist.gov/publications/drafts/800-181/sp800_181_draft.pdf

[ii] *Millennials surpass Gen Xers as the largest generation in U.S. labor force,* Richard Fry, May 5, 2015, http://www.pewresearch.org/fact-tank/2015/05/11/millennials-surpass-gen-xers-as-the-largest-generation-in-u-s-labor-force/