CompTIA®

The Computing Technology Industry Association
Subcommittee on Information Technology of the House Oversight and Government Reform Committee Hearing Testimony: "Reviewing Federal I.T. Workforce Challenges and Possible Solutions"
April 4, 2017

Introduction to CompTIA

We commend the Subcommittee on Information Technology of the House Oversight and Government Reform Committee for holding this hearing to solicit input regarding federal information technology (IT) workforce challenges and solutions, particularly in cybersecurity and as it relates to industry certifications.

CompTIA is a non-profit, high-tech trade association with approximately 2,000 member companies, 3,000 academic and training partners, and over 100,000 registered users.

CompTIA is the second largest IT certifying body in the world with more than two million vendor-neutral certifications issued globally. The CompTIA certifications most commonly recommended or required by federal agencies (CompTIA A+, CompTIA Network +, CompTIA Security+, and CompTIA Advanced Security Practitioner) are International Standard ANSI/ISO/IEC 17024 certified. [1]

Through all our activities, CompTIA is dedicated to advancing industry growth and workforce development through educational programs, market research, networking events, professional certifications, and public policy advocacy.

[1] In March, CompTIA unveiled a new exam to this suite of offerings: CompTIA Cyber Security Analyst or the CSA+ certification, which offers broad-spectrum validation of knowledge and skills required to configure and use cyber-threat detection tools, perform data analysis and interpret the results to identify vulnerabilities, threats and risks to an organization.

CompTIA welcomes the opportunity to discuss the federal workforce amidst a world defined by digitization and interconnectivity. Shortcomings in IT and cybersecurity expertise and experience make for an ever-more precarious situation. Government and the private sector alike have a challenge: to have in place the right skilled workforce to utilize technology, enhance productivity, and mitigate and manage security threats. We would like to share with you CompTIA's experience in working with the Federal government to enhance IT workforce skills; why we believe that workforce certifications fill a vital role in skilling the federal workforce; and what creative solutions for ensuring we have a skilled and able federal workforce are currently being discussed.

Helping to Establish Frameworks and Knowledge through Public-Private Partnerships

In many ways, the creation of CompTIA certifications, and those of many of our bretheren certifying bodies, have established a *de facto* framework for cybersecurity providing a pathway from entry-level to expert. For example, nearly a half million people are CompTIA Security+ certified. Cyber is also a crucial component of foundational IT certifications like CompTIA A+ and Network+. And CompTIA recently introduced Cyber Security Analyst (CSA+) to address the growing importance of big data analytics in cyber defense.

CompTIA exams are refreshed continually and undergo a complete rebuild every three years. They include practical knowledge based and performance based (simulation) questions that require test takers to have the knowledge they need to fill job roles. For credentials to remain valid after three years IT pros must commit to continuing education to prove their knowledge is up to date with the latest trends.

As the number of CompTIA certification holders has grown, we have sought to share and translate many of the lessons learned in creating and deploying these certifications with government as it has sought to create frameworks and standards to train and validate government employee skills in IT and cybersecurity.

To summarize, certifications are used to help professionalize the cyber workforce and help provide a common lexicon of the skills needed across the public and private sector. To this end, CompTIA would like to make the Committee aware of effective strategies and programs that are currently being used to promote public and private sector cooperation in ensuring a robust and high-skilled IT workforce.

The Department of Defense (DoD) has worked closely with the training and certification community to consistently up-skill workers. Many certification organizations have participated in the 8570[2] and successor 8140[3] initiatives. These initiatives, which require DoD personnel and contractors with information assurance titles (as defined by DoD) to have certain cybersecurity certifications, are vital for the U.S. Government workforce. This requirement ensures individuals are trained and certified in the skill sets required by their job. DoD's cyber workforce management strategy not only enhances our national security and ensures value from taxpayer investments in IT training, but it also assists DoD in meeting its IT/cybersecurity personnel retention goals. DoD training and certification programs have also supported the consistent goal across several administrations to help our veterans transition their skills to civilian employment once their military service has ended.

The DoD model has been so successful that CompTIA encourages the U.S. Government to lead by example and encourage other federal civilian agencies to adopt similar comprehensive programs. Related to this, CompTIA encourages Congress to review and consider updating the Government Employees Training Act (GETA)[4] to ensure that all federal government agencies have the flexibility needed to use resources allocated for IT training to pay for industry-recognized certifications where appropriate. It has been demonstrated through research individuals in training learn and retain more when they understand a certification exam will be required at the end of the process.

We also know the U.S. Government relies on the use of industry-recognized certifications for professional development. This is evidenced by the Department of Homeland Security's (DHS) National Initiative for Cybersecurity Careers and Studies (NICCS) portal, which highlights that certifications play a large role in getting people the skills they need to enter the cyber workforce.

Further, the FY16 Omnibus Appropriations Bill included the Federal Cybersecurity Workforce Assessment Act, directing the federal government to take stock of the certifications held by the

[2] DoD 8570.01-M, Information Assurance Workforce Improvement Program, December 19, 2005 (with updates)
[3] DoD Directive, Number 8140.01, August 11, 2015
[4] Title 5, U.S. Code, Ch. 41, Sec 4100

existing cyber workforce to determine what skills may be missing. We understand implementation is underway and encourage the Committee to conduct oversight of these assessments and to provide federal agencies with the resources needed to implement any mitigation plans proposed to address skills gaps and the absence of certifications.

The National Initiative for Cybersecurity Education (NICE) is also a critical element to properly training the nation's workforce. As you may know, NICE is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. CompTIA worked with NIST to map our certifications to the NICE workforce framework categories. We have provided as an appendix, a visual representation of that mapping to present a clearer picture of how CompTIA certifications validate cyber knowledge and skills categorized in the NICE framework. Significantly, the DoD 8140 directive aligns job roles with the NICE framework.

CompTIA has also worked closely with the National Institute of Standards and Technology (NIST) to provide real-time information concerning the location of qualified IT workers. To that end, in 2015, CompTIA, in partnership with Burning Glass Technologies, received a three-year grant from NIST to develop an interactive cyber jobs heat map that shows the demand for and availability of critical cybersecurity jobs (mapped to the NICE Framework) across the nation. The project, which is being funded through NICE, provides data to help employers, job seekers, policy makers, training providers, and guidance counselors meet today's increasing demand for cybersecurity workers. The heat map was released in October 2016 under the name **CyberSeek.org**. A few high level data points:

- According to CyberSeek, every year in the U.S. there are 128,000 openings for Information Security Analysts, but only 88,000 workers currently employed in those positions – a talent shortfall of 40,000 workers for cybersecurity's largest job.
- There are 220,000 additional openings requesting cybersecurity-related skills, and employers are struggling to find workers who possess them. Jobs requesting cloud security skills, for example, remain open 96 days on average – longer than any other IT skill.

Understanding the types of cyber jobs that are in demand and where supply falls short is vital to ensuring that we are preparing individuals with the right skills for the jobs in demand.

The Value of Training and Certification

We also believe it is critical we in the certification industry constantly gauge the value and relevancy of certifications. To that end, CompTIA conducted research on managers' perceptions of the importance of testing after training. Our research on this topic targeted DoD, which we believe has set the "gold standard" for building a robust IT and cybersecurity workforce. CompTIA's Military Career Path Study found that 74 percent of active duty military personnel with staff management responsibilities classified testing after training to confirm knowledge gains as "very important."[5] Further, these managers reported that testing after training also helped to set a baseline of expertise among staff, provide career path guidance, improve the performance of a team, retain talented staff, and evaluate staff for promotions or career advancement.[6]

According to a study conducted by the International Data Corporation (IDC) and sponsored by CompTIA, candidates and staff with CompTIA A+ and CompTIA Security+ certifications perform better than staff that is not certified. According to the research, certified employees are: (1) more confident; (2) more knowledgeable; (3) reach job proficiency more quickly; (4) more reliable; and (4) perform at a higher level.

When IT professionals are confident in their abilities, they are more likely to be forward thinking, proactively anticipate issues, and solve problems before those problems impact organizational performance. Further, certified professionals are 85 percent more likely to believe they have the knowledge and skills needed to successfully fulfill their jobs.[7] As a result, these certified security professionals are better positioned to properly assess risks, design and implement interventions, and correct policy weaknesses.

Because most of today's hiring environments prioritize experience above professional credentials, it is also important to note that CompTIA's research has found that after ten years of security experience or support experience, certified staff has between 20 and 25 percent more core domain knowledge than those with the same experience who are not certified. Once on the

[5] CompTIA 2014 "Military Career Path Study: Assessing the Role of Training and Certifications."
[6] Id.
[7] CompTIA 2014 IT Support and Security Performance Study: The Impact of CompTIA Certifications on Organizational Performance.

job, certified IT professionals have also been found to perform up to 53 percent better than those without certification in critical, job-related activities.[8]

Further, certifications help to put program managers at greater ease with the capabilities of their staff. Ninety-three percent of human resources (HR) executives believe certifications are beneficial, as they offer a competitive edge in the job market, heightened career advancement opportunities, and increased value to employers and their organizations.[9] According to employers, the top benefits of IT certification are: (1) the ability to understand new or complex technologies; (2) higher productivity; and (3) more insightful problem, solving.[10] In addition, CompTIA has found that roughly 8 in 10 hiring managers say it is challenging to find the right candidates with the right skill sets to fill vacant IT positions and verifying job candidates' credentials can be a challenge.[11]

Creating a Pipeline for IT and Cybersecurity Talent

While CompTIA is best known for validating the skills of the existing and aspiring IT and cybersecurity workforce, we recognize a steady talent pipeline is needed to ensure the IT and cybersecurity workforce of the future. Our nation is struggling to fill job openings with roughly 1 million open IT job postings each year. This is not to say that every job posting must or will be filled, but many of these are desirable positions, especially as several of these job vacancies have an average starting salary of $50,000 with growth into the six figures.[12]

We believe IT/cybersecurity should be given strong consideration as a profession for individuals looking to enter or re-enter the workforce or make a career change. This is especially true because a formal degree is not the only entry point for a successful career in IT/cybersecurity. If formal education is needed, very often a two-year community college degree will suffice. There are also a number of training programs that are not tied to academic institutions, but offer industry-recognized certifications to start individuals on career pathways in cybersecurity. To clarify, there is a varying level of cyber worker. The "cyber ninja," who is at the top of the IT/cyber workforce pyramid, may require a lot more training and formal education. However,

[8] Id.
[9] CompTIA 2015 IT Careers Blog: Four Reasons HR Execs Love Certifications.
[10] Id.
[11] Id.
[12] Source: Burning Glass Technologies.

many cybersecurity and IT jobs do not require a four-year college degree and present solid employment opportunities.

We are aware of efforts at the federal level aimed at creating tuition reimbursement for cybersecurity degrees. We ourselves have put forward a proposal, to be included in the FY18 National Defense Authorization Act (NDAA), for a "Service to Cyber Warriors" program that would provide financial assistance in the form of a stipend, available to veterans and members of the Armed Forces without any requirement of prior IT experience, industry-recognized certification, or advanced degree. Under our proposal, up to $5,000 in stipend funds may be made available to a participant to cover the expenses of IT training, training materials, industry-recognized certification exam voucher fees, and other employment seeking services.

We acknowledge that creating a workforce pipeline is only part of the problem; the federal government also faces significant retention challenges. Due to our extensive work with DoD, we know the Department's ability to remain competitive with the private sector in compensation can impact retention goals. Therefore, we are also proposing a bonus payment of up to $10,000 for Program participants who agree to enter into a contract service agreement for full-time employment in a cyber work role at a federal, state, or local government agency for a period of time to be specified by the Secretary of Defense.[13]

A number of similar proposals have recently been introduced in Congress. For example, CompTIA has supported the State Cyber Resiliency Act introduced in the House by Representatives Kilmer (D-WA) and Comstock (R-VA) and in the Senate by Senators Warner (D-VA) and Gardner (R-CO). On the workforce front, this legislation encourages states to develop cyber resiliency plans to fulfill the essential functions of mitigating talent gaps in the state government cybersecurity workforce, enhancing recruitment and retention efforts, and bolstering the knowledge, skills, and abilities (KSAs) of state government personnel to protect against cyber threats and vulnerabilities. Further, the bill allows states to use implementation grant funds to establish programs, such as scholarships or apprenticeships, to provide financial assistance to state residents who pursue formal education, training, and industry-recognized

[13] Priority will also be given to those who agree to seek employment in a state with low cybersecurity workforce supply and high cybersecurity workforce demand, as identified by the National Institute of Standards and Technology (NIST) (via CyberSeek).

certifications for careers in cybersecurity as identified by NICE and commit to working for state government for a specified period of time (based on Virginia's successful Cybersecurity Public Service Scholarship Program).

Also, recently introduced are the DoD Cyber Scholarship Program Act and the Cyber Scholarships Opportunity Act. CompTIA supports the overarching goal of these legislative proposals to build a robust cybersecurity workforce. We believe these proposals could only be strengthened by recognizing training and industry-recognized certifications as yet another pathway to upskilling the federal workforce. We believe the federal government can continue to demonstrate leadership and work towards swifter and more cost-effective achievement of its IT/cyber workforce goals by prioritizing resources for training and industry-recognized certifications. CompTIA believes such initiatives could have tremendous impact among members of the federal workforce who are not enrolled in four-year institutions.

Finally, CompTIA also supports apprenticeships and vocational models for building out our nation's IT/cybersecurity talent pipeline. We believe the real-world experiences that can be gained through these types of apprenticeship and vocational positions can only enhance an individual's training for a successful career in IT/cybersecurity. We are now working with a number of House and Senate offices on a legislative proposal, called the Championing Apprenticeships for New Careers and Employees (CHANCE) in Tech Act, to scale up the number of tech apprenticeships in our nation.

Conclusion: The IT Skills Gap

All of these proposals address the issue of a skills gap. According to the Bureau of Labor Statistics, by 2022, more than 25% of U.S. workers will be 55 years old or older, up from 14% in 2002. In the sphere of IT, nearly 800,000 workers are expected to retire through 2024.[14] And even within the federal government, according to the Office of Personnel Management (OPM), from 2006 through 2015 there were nearly 24,000 retirements from the federal civilian workforce of IT management personnel.[15]

[14] CompTIA Research Brief: "Assessing the IT Skills Gap", March 2017

[15] United States Office of Personnel Management, "Executive Branch Retirement Statistics: Fiscal Years 2006-2015."

Across the board, we are seeing IT talent leave and a shortfall of talent taking their place. While the notion of a skills gap is a seemingly straightforward concept, below the surface, there are many nuances to the story. At the most basic level, skills gap can be characterized as the variance between the performance employers desire from their workforce and what workers can or choose to deliver. Things get murky when skills gap discussions venture into other workforce challenges, such as gaps in labor supply, pipeline, locations, or generational. For example, what may be thought of as a skills gap by an employer may in fact be a difference in millennial work styles. Obviously, knowing what to fix must precede discussions of how to fix it.

In closing, as this Committee considers innovative ways in which to address meeting a skills gap in the federal workforce, it should consider the various nuances that we have outlined. Generational, financial, and career path considerations are all equally as relevant in the federal workforce as it is in the private sector.