Testimony of
Dan Waddell
Managing Director, North America & Director of U.S. Government Affairs
(ISC)²

Before the United States House of Representatives
Subcommittee on Information Technology of the
Committee on Oversight and Government Reform

"Reviewing Federal I.T. Workforce Challenges and Possible Solutions"

April 4, 2017

Chairman Hurd, Ranking Member Kelly, and distinguished members of the Committees, let me begin by thanking you for inviting me to speak on this very important issue. On behalf of (ISC)², we look forward to working with you in the coming years to help ensure our country is safe, secure, and resilient against cyberattacks and other risks.

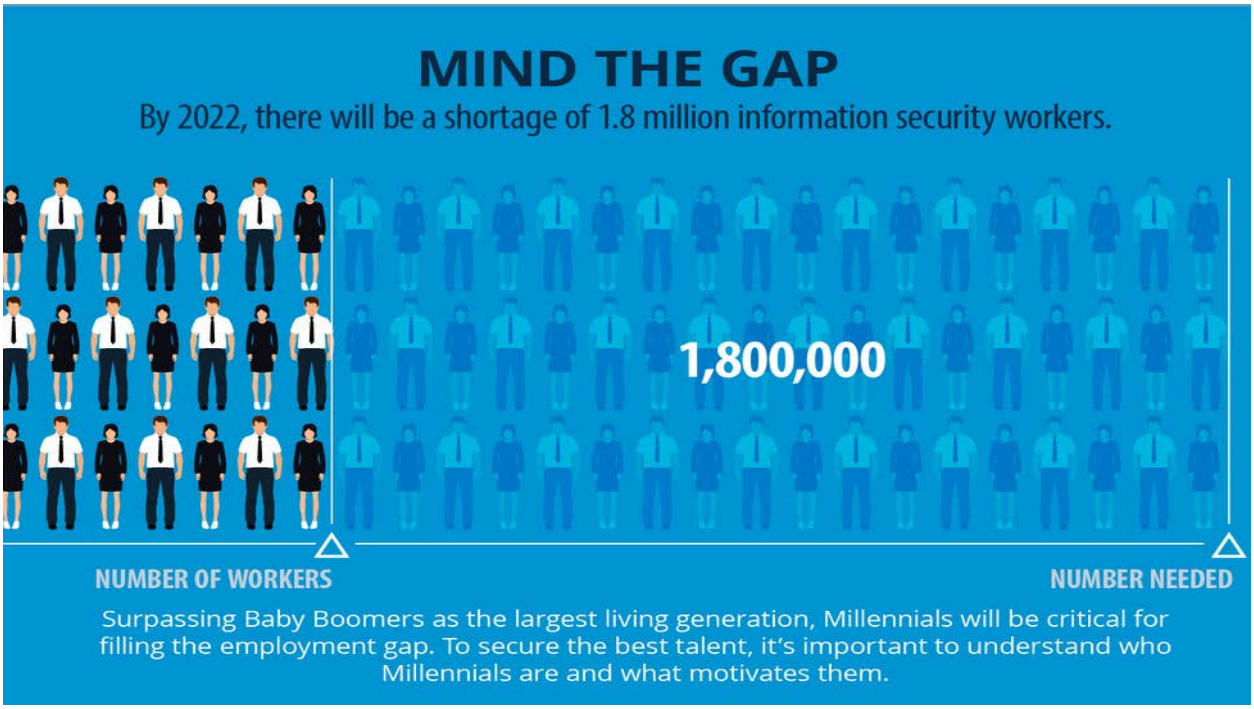
As a matter of introduction, (ISC)² stands for the International Information System Security Certification Consortium. We are the largest nonprofit membership body of certified cyber, information, software and infrastructure security professionals, with over 123,000 members worldwide – of which many are currently employed at or contracted by our federal government. Known for our Certified Information Systems Security Professional, the CISSP is the industry-leading certification for information security professionals. When employees earn their CISSP or any of our other certifications, it shows they have the knowledge and skills of true experts. Ideally, through our continuing professional education requirements, they will be qualified throughout their lifetimes. Through our certifications, our training and education offerings, and our research, internet safety and scholarship programs, we encourage cybersecurity students and professionals to start with us, stay with us and grow with us.

Since 1989, (ISC)² has provided a solid foundation for the life-long development of the industry's top talent. As a professional membership community, our role is to inform and educate wherever there is a void, in order to better safeguard people and their information assets. As an advocate for the professionalization of the cybersecurity workforce, our role is to be the voice of our members and the broader cybersecurity profession. Our ability to effectively fulfill these roles ultimately determines the success of our mission and our vision – to inspire a safe and secure cyber world.

However, accomplishing this vision is made more difficult when there is a lack of qualified cybersecurity professionals. Recently, (ISC)² and our charitable trust - the Center for Cyber Safety and Education – conducted the largest study of the cybersecurity profession – the Global Information Security Workforce Study (GISWS). The 2017 version of this bi-annual study took place from June through September 2016 via a web-based survey. Over 19,000 cybersecurity

professionals from 170 nations responded. Since its first release in 2004, this study gauges the opinions of cybersecurity professionals, and provides detailed insight into important trends and opportunities within the profession. It aims to provide a clear understanding of pay scales, skills gaps, training requirements, corporate hiring practices, security budgets, career progression and corporate attitudes toward information security that is of use to companies, hiring managers, industry professionals – and most importantly, for you here today.

This survey projects that the gap between available qualified professionals and unfilled positions will widen on a global scale to 1.8 million by 2022, as illustrated in the graphic below.



We will be releasing the U.S. Government-specific results on May 9th at our annual Washington, D.C. event - CyberSecureGov, and will include data from over 1,600 U.S. Government respondents.

So what can we do collectively to solve this crisis?

Recently, the (ISC)² executive management team gathered recommendations that we believe will be critical to the success of the cybersecurity workforce. Specifically, during a gathering in December 2016, members of (ISC)²'s U.S. Government Advisory Council hosted former Federal Chief Information Security Officer Greg Touhill and a group of federal agency CISOs and executives to discuss what was necessary to ensure the continuation of progress during the presidential transition. As a result of that discussion, we offered the following recommendations:

- ***Consider the Progress Already Made.*** Cybersecurity is a bi-partisan issue. Critical work has been done over the last 8 years to advance the cybersecurity workforce. (ISC)² was a strong advocate of the Cybersecurity National Action Plan (CNAP) which led to the creation of the first federal CISO position under the previous administration. That is why we recommend the *reinstatement of both the federal Chief Information Officer (CIO) and CISO positions, but with greater authority.* The next federal CIO and CISO must have the ability to positively affect change, have a depth of experience in both the technical and managerial aspects of cybersecurity, and must be advocates for effective, holistic cybersecurity solutions that include people, process and technology as equally essential components.
- ***Harden the Workforce.*** Everyone must learn cybersecurity. We have to break the commodity focus of simply buying technology and stopping there, without focusing on training all users. 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.
- ***Incentivize Hiring and Retention.*** 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's (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, 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.
- ***Prioritize investment in Acquisition, Legal and Human Resources (HR) Personnel.*** Acquisition, Legal and HR professionals are essential players within the federal cybersecurity ecosystem. They need to be educated on both the needs of the customer and the nuances of the cyber workforce in order to develop accurate Requests for Proposals (RFPs) and job descriptions that will result in quality hires and the procurement of secure products and systems.
- ***Prevent Getting Lost in Translation.*** The government needs effective communicators who can translate technical risk to business leaders in order to improve communications between cyber personnel and the boardroom. Effectiveness of the CISO role in the future will depend upon a "translation" layer of personnel that must be established and trained. The government realized this in changes made to OMB Circular A-123 which now calls for a Chief Risk Officer at each agency. Efforts to align technology risk with mission and business strategies should leverage this OMB initiative.
- ***Civil Service Reform.*** The civil service system is broken and does not meet the government's needs. 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 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.

- ***Compliance Does Not Equal Security - Embrace Risk Management.*** According to NIST, the definition of resilience is "the ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs." In the government's quest for cyber resiliency, a risk management perspective will be essential.
- ***A Standard Cyber Workforce Lexicon.*** In November 2016, NIST released draft NIST Special Publication 800-181 titled, "NICE Cybersecurity Workforce Framework (NCWF)," and is currently reviewing public comments. (ISC)² is working to align our certifications with this new framework which represents years of collaboration across government, industry and academia. According to NIST, the "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.

(ISC)² also has a number of programs both internally and through our partners that can help address the workforce shortage. I will briefly mention two below.

1. **Associate of (ISC)².** The Associate of (ISC)² allows those just starting out in the information security workforce to demonstrate their competence in the field. Associates have passed a rigorous (ISC)² certification exam, proving their cybersecurity knowledge, and maintaining their continuing professional education (CPE) requirements while working toward completing the experience requirements to become fully certified. Exam costs here in the U.S. currently range from $250 to $599.
2. **Virginia Veteran Cyber Training Pilot.** This initiative is a unique cyber training collaboration between the Commonwealth of Virginia and private sector leaders, including Cisco, Amazon Web Services (AWS), (ISC)² and the Institute for Veterans and Military Families' Onward to Opportunity program (O2O). The initiative provides a free, cyber training program for veterans living in Virginia who are interested in careers in the cyber industry.

Through these recommendations and the programs we offer, (ISC)^2 hopes to establish an open avenue of communication with you, your staff and others in Congress as we all work towards strengthening cybersecurity throughout the federal government both now and in the future. We see this time of transition as an opportunity for our members to be a stabilizing force during an intrinsically uncertain process. (ISC)^2 would like to offer its ongoing support to you and the other organizations represented here today by providing resources, research and community.

Dan Waddell, CISSP, CAP, PMP, (ISC)² Managing Director, North America Region

Mr. Waddell is responsible for managing operations in the North America Region, which primarily focuses on supporting our U.S. and Canadian members, customers and strategic partners. He also leads all Government Affairs activities in North America and is the primary (ISC)² official responsible for interacting with public sector entities (i.e. federal, state and local governments), major corporations, universities and other higher education institutions and professionalization organizations throughout the U.S. and Canada. Mr. Waddell serves as the principal point of contact for various trade associations, public interest groups and other entities focused on information security and information security workforce issues. He has 24 years of experience in information technology and information security, with 20 of those years in management.

My roots in IT started as a self-taught PC technician at SAIC in 1993, where I learned the craft through building computers and software images at home, in the work lab, and at school. I moved into management at SAIC in 1997 and began expanding my knowledge up the stack into network administration. I was inspired to join the information security workforce after 9/11, as I worked to assist the Department of Defense to help improve cyber resiliency across a number of complex systems such as Army Knowledge Online (AKO) – which at its peak was considered by many to be the world's largest corporate intranet. I also spent several years in consulting at firms such as Deloitte where I provided expertise to federal civilian agencies to help them solve cybersecurity related issues. Today, as an experienced director having led several successful cybersecurity programs and departments overseeing multi-million dollar budgets and contracts, I am a trusted

advisor on a number of multiple disciplines and skill areas including workforce, career development, CISO/CSO advisory services, program management, cloud security, security authorization, privacy, data loss prevention, regulatory compliance, threat and vulnerability assessments, penetration testing, social engineering, social media, incident response, disaster recovery/business continuity, risk management, training, education and certification.

Mr. Waddell graduated summa cum laude from Strayer University with a B.S. in Computer Information Systems. He has been a featured guest speaker on information security issues on both TV and radio shows such as "NBC News4 Midday", "Government Matters" and "Federal News Radio" in Washington D.C., in addition to several information security conferences across the United States and Canada. He is currently a Fellow at the Institute of Critical Infrastructure Technology (ICIT), a non-partisan think-tank based in Washington, D.C. that acts as a conduit between the legislative community, technology providers and federal agencies. Mr. Waddell also chairs both the (ISC)² U.S Government Advisory Council and the U.S. Government Executive Writers Bureau, and received the (ISC)² President's Award in 2013. You can find him on Twitter at @danwaddellcissp.