Written testimony of Debora Plunkett, Strategic Advisory Board Member of the International Consortium of Minority Cybersecurity Professionals, for the hearing of the Subcommittee on Information Technology of the Committee on Oversight and Government Reform titled "Reviewing Federal IT Workforce Challenges and Possible Solutions" Tuesday, April 4, 2017 2:00PM

Chairman Hurd, Ranking Member Kelly, and distinguished Members of the Subcommittee, I am pleased to appear today to discuss the challenges to developing, recruiting, and retaining the federal government's IT, and specifically cybersecurity, workforce with a specific focus on leveraging the capacity of diverse talent to meet these needs.

Our testimony today will highlight the challenges being faced across the public and private sectors in recruiting and retaining cybersecurity talent. These challenges are compounded for diverse populations, which face issues with career advancements for existing diverse practitioners and retention challenges that also exist in keeping diverse talent once they are recruited. We will also discuss the role and the progress that grassroots non-profits like the one I'm here representing today, the International Consortium of Minority Cybersecurity Professionals (ICMCP), have made in closing what we have called, "The Great Cybersecurity Diversity Divide." Ultimately, these challenges extend across government and private sector, with scarce talent and high demand, making it even more critical to focus efforts on increasing capacity. As noted in the Cybersecurity National Action Plan and 2017 Budget, the goal remains "…to identify, recruit, develop, retain, and expand the pipeline of the best, brightest, and most diverse cybersecurity talent for Federal service and for our Nation." As noted in the January 2017 report entitled "Diversity and Inclusion: Examining Workforce Concerns Within the Intelligence Community" commissioned by the Intelligence Community Equal Employment Opportunity and Diversity Office, "(t)he value of increasing diversity, especially in underrepresented segments such as minority groups, women and persons with disabilities, expands the talent base and more accurately reflects analytic capabilities necessary to evaluate and meet mission requirements." Additionally, a 2014 CIA Diversity in Leadership study commissioned by the Director of the CIA, noted that "…a lack of diversity of thought and experience was identified by congressional committees and independent commissions as contributing to past intelligence failures. That diversity is mission critical is no longer a debatable proposition – if it ever was."

The Realities of the Cyber Threat Landscape

There is no doubt that cyber threats today touch on virtually every aspect of the lives of our citizens. As a nation, we are faced with pervasive cyber threats and vulnerabilities. Malicious actors, including those at nation-state levels, are motivated by a variety of reasons that include espionage, political and ideological beliefs, theft and financial gain. Increasingly, State, Local, Tribal and Territorial (SLTT) networks are experiencing cyber activity at a sophistication level similar to that seen on National networks. These forces are not expected to decrease but rather will continue apace,

The Realities of the Cybersecurity Workforce Diversity

According to Frost & Sullivan's 2017 International Information Systems Security Certification Consortium (ISC2) Global Information Security Workforce Study (GISWS) of over 19,000 information security professionals globally, across 170 countries, women represent only 11% of the total cybersecurity workforce despite a projected workforce shortfall of 1.5 million people during the next five years due to a lack of trained professionals. The percentage representation of African Americans and Hispanics in cybersecurity has been reported at approximately 12% combined, for both these groups. This data takes on added meaning when we consider the projected growth in the U.S. minority population over the next few decades where the Hispanic population is expected to grow to 28.8% of the US population and the African American population is expected to climb to almost 20% according to Census data reflecting population growth from 2014 – 2060.

This workforce shortfall should be of much consternation given that cybercrime and information theft, to include cyber espionage, are some of the most serious economic and national security challenges that the country faces. In fact, as we speak, there are discussions in this Congress regarding the potential role that Russia may have played in our recent Presidential elections. There is an urgent need for more capacity to address this, as well as other current-day cyber threats. It has also been reported that the under-participation by large segments of our society represents a loss of opportunity for individuals, a loss of talent in the workforce, and a loss of creativity in shaping the future of cybersecurity. Not only is it a basic equity issue, but it threatens our global economic viability, and even our democracy, as a nation.

The Roots of the Cybersecurity Workforce Diversity Starts in our Middle Schools and High Schools

The workforce shortfall and the growing diversity gap in the cybersecurity industry in the United States also reflects the broader challenge that the USA faces in science, technology, engineering and mathematics , or STEM, programs in our schools. Until we can get more students matriculating with STEM-related degrees, these challenges faced within the cybersecurity industry and overall information technology industry will persist. According to the PEW Research 'Fact Tank' Report of International Students in Math and Science, American 15-year-olds were ranked 38th out of the 71 countries included in the report. The results were only slightly more encouraging for our 8-year-olds, who were ranked 11th out of the 38 countries included. As a country, we have to be laser-focused on quality and retention in middle and high school STEM programs, as these formative years determine the future talent pipeline for the cybersecurity workforce. Strategies and programs are needed to provide significantly more apprenticeship opportunities as well as opportunities in colleges and universities, to include an infusion of federal resources to support everything from curriculum and faculty development to tuition support.

Mr. Chairman, our STEM imperative cannot be more urgent for minority students. The mandate is clear when we consider the projected growth of minority populations according to the census data and the reported labor trends citing the fact that over 90% of all jobs by 2030 will require information technology skills.

The Imperatives for Grassroots Organizations like ICMCP

Toward leading tangible and meaningful societal change, the International Consortium of Minority Cybersecurity Professional (ICMCP) was created in 2014, achieving formal 501(c)(3) Public Charity Non-Profit from the Internal Revenue Service (IRS) in July 2014 and with the expressed purpose of "Bridging The Great Minority Cybersecurity Divide."

The ICMCP is tackling this "Divide" by creating academic scholarship opportunities to attract more females and students of color into the career field. For existing minority cybersecurity practitioners, ICMCP is deploying strategic mentoring programs geared towards fostering the career growth of junior and mid-level practitioners into becoming the next generation of executive decision-makers. Studies by various groups to include Diversity, Inc. and Working Mothers among others, have underscored the importance of mentoring, sponsorship and employee affinity groups as key strategic components of successful diversity and inclusion programs and employee retention initiatives.

ICMCP has developed five key objectives to address the cybersecurity diversity divide:

1. Increase the number of scholarship, internship and employment opportunities for minority STEM students pursuing cybersecurity related disciplines at both the undergraduate and post-graduate levels.

2. Facilitate the increased attraction, retention, professional development and career advancement of qualified, skilled entry-level to senior-level minority cybersecurity professionals.

3. Promote community awareness of the cybersecurity industry and the opportunities within, for minority cybersecurity professionals.

4. Serve as THE voice and destination for issues related to cybersecurity career and industry developments impacting minority cybersecurity professionals.

5. Establish online and offline channels and "virtual centers" to gather and disseminate relevant information for minority cybersecurity professionals.

Toward fulfilling these five key organizational objectives, last year ICMCP accomplished the following due to the generosity of our sponsors,

- Awarded 10 Academic Scholarships @ $5K each
- Awarded 5 Certification vouchers (average $3K)
- Awarded 1 Executive Development stipend ($16K)
- Placed 12 interns in cybersecurity positions
- Matched 17 Protégés to Mutually Matched Mentors
- Assisted and facilitated the job placements of over a dozen minority cybersecurity professionals at various levels in several industries
- Implemented the first operational Security Operations Center (SOC) at an academic institution toward ensuring students graduate with hands-on skills to augment their classroom learning.

So far in 2017, ICMCP has:

- Awarded over $100K in academic scholarships
- Awarded at least 10 certification vouchers (ISC2, CompTIA, SANS, ISACA, IAPP)
- Coordinated the placement of 6 interns and 3 job-seekers

We should also mention several ongoing and very noteworthy government-led initiatives, many with diversity underpinnings also tackling the "Great Minority Cybersecurity Divide" which include:

GenCyber
The National Security Agency's GenCyber program, co-sponsored by the National Science Foundation, sponsors cybersecurity summer camps for students and teachers at the K-12 level. The goals of the GenCyber program are to help increase in diversity in the cybersecurity career field, help students understand correct and safe on-line behavior and to improve the teaching methods for delivering cybersecurity content in the K-12 curricula. This year the program sponsored 130 GenCyber camps and reached nearly 5,000 students and 1,000 teachers across the nation.

The Consortium Enabling Cybersecurity Opportunities and Research (CECOR)
The Consortium Enabling Cybersecurity Opportunities and Research (CECOR) funded by the Department of Energy is a collaborative effort among thirteen colleges and universities and two national laboratories to develop a K-12 pipeline for the cybersecurity workforce.

CyberCorps Scholarship for Service (SFS) Program
SFS is a program designed to increase and strengthen the cadre of federal information assurance professionals that protect the government's critical information infrastructure. This program provides scholarships that may fully fund the typical costs incurred by full-time students while attending a participating institution, including tuition and education and related fees. The scholarships are funded through grants awarded by the National Science Foundation.

But this is clearly not enough. To make significant progress in developing and employing the cybersecurity capacity our nation needs, we need to be filling over 200,000 cybersecurity jobs annually according to the Frost and Sullivan ISC2 GISWS Report and to make these opportunities available to diverse candidates.

Diversity is the Strategic Imperative
Mr. Chairman, several studies have proven that diverse teams win and specifically in the private sector, diversity has been shown to positively impact bottom line revenues. In fact, recent reports are showing that every incremental percentage point in African American and Hispanic representation at NASDAQ-listed tech companies is linked with a three-percentage-point increase in revenues. If the racial/ethnic diversity of tech companies' workforces reflected that of the engineering talent pool, the sector at large could generate a 20 – 22 percent increase in revenue—an additional $300 – $370Bn each year. Companies with above-median Hispanic representation (currently standing at roughly 5 – 6 percent of the technical workforce) are linked with annual revenues that are 40 percent higher than companies that fall below the median in Hispanic representation.6 The links between African American representation and revenues were also positive, yet did not show statistical significance.

There is also a linkage between racial/ethnic diversity and operating margins - every one percentage point increase in racial/ethnic diversity at a tech company is linked with 0.3 – 0.4 percentage point increase in operating margins. Extrapolating to the tech sector achieving levels of racial/ethnic diversity that reflect the talent marketplace would be linked with $6 – 7Bn in additional operating earnings industry-wide, or roughly a 2 – 3 percent increase in total industry earnings.

These links between diversity and financial performance are not unique to the tech industry—a range of studies conducted in other industries support them. For instance, research published in the American Sociological Review found that firms with high levels of racial/ethnic diversity have more than 98 percent higher sales revenue, serve over 54 percent more customers, are roughly 33 percent more likely to have above-average market share, and are nearly 30 percent.

Our analysis is supported from the commercial sector, by the well-known consulting firm of McKinsey & Company which conducted a 2015 study of 366 public companies across a range of industries in the United Kingdom, Canada, the United States, and Latin America. The resulting analysis of the 366 companies revealed a statistically significant connection between diversity and financial performance. The companies with the highest gender diversity were 15 percent more likely to have financial returns that were above their national industry median, and the companies with the highest racial/ethnic diversity were 35 percent more likely to have financial returns above their national industry median. The correlation does not prove that greater gender and ethnic diversity in corporate leadership automatically translates into more profit—but rather indicates that companies that commit to diverse leadership are more successful

Conclusion

In closing Mr. Chairman, there are several good efforts underway to address cybersecurity capacity writ large, some of which also tackle the problem we have titled the "The Great Minority Cybersecurity Divide". Progress is being made but more must be done, and with a sense of urgency commensurate with our understanding of the capabilities and intentions of nation states as well as other bad actors. Sadly however, with over 200,000 unfilled jobs in cyber each year, with the average representation of women in the cybersecurity industry averaging barely 10% for the past few years, and analogous to the combined representation of African Americans and Hispanics with one or two percentage points, there is much more that can be done and that must be done when we consider the projected minority population growth and trends in the labor market.

Thank you for the opportunity to testify, and we look forward to your questions.

Committee on Oversight and Government Reform
Witness Disclosure Requirement — "Truth in Testimony"

Pursuant to House Rule XI, clause 2(g)(5) and Committee Rule 16(a), non-governmental witnesses are required to provide the Committee with the information requested below in advance of testifying before the Committee. You may attach additional sheets if you need more space.

Name: Debora A. Plunkett

1. Please list any entity you are testifying on behalf of and briefly describe your relationship with these entities.

Name of Entity	Your relationship with the entity
ICMCP	Member, Strategic Advisory Board, International Consortium for Minority Cybersecurity Professionals (ICMCP)

2. Please list any federal grants or contracts (including subgrants or subcontracts) you or the entity or entities listed above have received since January 1, 2015, that are related to the subject of the hearing.

Recipient of the grant or contact (you or entity above)	Grant or Contract Name	Agency	Program	Source	Amount
N/A	N/A	N/A	N/A	N/A	N/A

2. Please list any payments or contracts (including subcontracts) you or the entity or entities listed above have received since January 1, 2015 from a foreign government, that are related to the subject of the hearing.

Recipient of the grant or contact (you or entity above)	Grant or Contract Name	Agency	Program	Source	Amount
N/A	N/A	N/A	N/A	N/A	N/A

I certify that the information above and attached is true and correct to the best of my knowledge.

Signature Debora A Plunkett Date: 31 March 2017

Debora A. Plunkett

Debora Plunkett is a cybersecurity leader with more than 30 years of experience. Culminating a career of U.S. federal service in 2016, she currently is Principal of Plunkett Associates LLC, a cybersecurity consulting business. Additionally, she serves as an Adjunct Professor at the University of Maryland University College Graduate School in the Cybersecurity program. She also serves on several boards.

As a federal senior executive, Ms. Plunkett served first as the Deputy Director and thereafter for over four years as the Director of the National Security Agency's Information Assurance Directorate. As the leader of NSA's cyber defense, cryptography and information systems security missions, she directed thousands of personnel across NSA's worldwide presence and managed a multi-million-dollar budget. Her efforts enabled continuous innovation and development of strong security solutions and policies for the protection of the classified communications of the United States government, serving the needs of a wide range of consumers from the White House to the war fighter.

Ms. Plunkett also served as the first Senior Advisor to the Director of the National Security Agency (NSA) for Equality where she led efforts to develop and deliver solutions to improve equality, inclusion and diversity for the highly technical NSA workforce. Her efforts resulted in the identification and implementation of new strategies to address systemic issues. In one year, her breakthrough leadership resulted not only in new NSA policies and processes, but also extended to the broader Intelligence Community (IC) where the Director of National Intelligence (DNI) mandated two of her initiatives for the entire IC.

Ms. Plunkett has significant executive experience in working with industry and at the senior-most levels of the U.S. government. She served as Director on the National Security Council at the White House in the Administrations of Presidents William Clinton and George W. Bush where she contributed to the development of national cybersecurity policy.

Among her many awards are the ranks of Meritorious Executive in the Senior Cryptologic Executive Service by President George W. Bush in 2007 and Distinguished Executive by President Barack Obama in 2012. In 2015 Debora was recognized with the Intelligence Community Equal Opportunity and Diversity Exemplary Leadership Award from the Director of National Intelligence and the Exceptional Civilian Service Award from the NSA Director.

A graduate of Towson University with a Bachelor of Science degree, Debora also earned an MBA from Johns Hopkins University, and a Master of Science in National Security Strategy from the National War College. She also completed the Harvard Law School program in Conflict Management and Negotiations, and the Leadership at the Peak program at the Center for Creative Leadership. She values remaining current on best practices in leadership.