STATEMENT FOR THE RECORD OF

JULIET OKAFOR, JD, VICE PRESIDENT OF GLOBAL BUSINESS DEVELOPMENT, FORTRESS INFORMATION SECURITY
BEFORE THE U.S. HOUSE OF REPRESENTATIVES HOMELAND SECURITY SUBCOMMITTEE ON
CYBERSECURITY AND INFRASTRUCTURE PROTECTION

"CHALLENGES OF RECRUITING AND RETAINING A CYBERSECURITY WORKFORCE"

September 7, 2017, 2:00 PM | HOUSE CAPITOL VISITOR CENTER (CVC) ROOM 210 House Homeland Security

Thank you Chairman Ratcliffe, Ranking Member Richmond and Members of the House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection. I am pleased to appear before you today to discuss the challenges of addressing the severe "people problem" in addressing the advancing threat to our nation's critical infrastructure. Technology alone cannot bridge the increasing skills gap our federal government continues to face in recruiting and retaining highly skilled cybersecurity talent. Similar to the private sector, it is our belief that the federal government must take a more innovative approach to the recruitment and retention of our future cyber workforce.

My name is Juliet Okafor, JD, Vice President of Business Development for Fortress Information Security and Strategic Advisory Board Member for the International Consortium of Minority Cybersecurity Professionals (ICMCP). I am the first Black and Female employee of Fortress Information Security, a minority-owned, cyber risk intelligence and management startup based in Orlando Florida. Fortress was founded in

2015 by two serial entrepreneurs, who sought to apply practical business intelligence to address the most complex and emerging challenges across IT, OT, and Third-Party Risk Management, facing the global critical infrastructure. Our approach to the market – bundling analytics-enabled security risk orchestration technology, risk governance and people stemmed from the constant concern reported by CISO's of the world's largest organizations about their ability to hire skilled security staff to fill critical technical security roles.

In May 2016, I joined the International Consortium of Cybersecurity Professionals as the first Female Co-Chairwoman of the Strategic Advisory Board and Chair of the Fundraising Committee for ICMCP. I lead strategic planning and roadmap development for strategic initiatives, partnerships and community outreach. In this role, I spend much of my time listening to the efforts experienced by the largest global corporations, small businesses and educational institutions regarding building a talented, diverse and innovative cyber workforce. Then identifying opportunities, programs, tools and processes that enterprises can leverage to expand diversity and inclusion programs.

ICMCP's the key organizational objectives are to:

1. Increase the number of female and minority students pursuing cybersecurity related disciplines at both the undergraduate and post-graduate levels by funding scholarships opportunities.
2. Facilitate the career advancement of existing member cybersecurity practitioners through mentoring and grants leading to advanced degrees and/or professional certifications in the field of cybersecurity.
3. Promote public awareness of cybersecurity and the opportunities for minorities in the profession.
4. Function as a representative body on issues and developments that affect the careers of Minority Cybersecurity Professionals.
5. Establish a mechanism for gathering and disseminating information for Minority Cybersecurity Professionals.

In my testimony today, I will highlight the challenges being faced across the public and private sectors in recruitment and retention of cyber security talent. These challenges are compounded for diverse populations, which faces 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 efforts and progress made by large and small enterprises, and grassroots non-profits like the organizations I represent today, Fortress Information Security and ICMCP, have made in addressing the cyber security industry's largest and critical vulnerability – the human factor.

Our research shows that 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." Additionally, a 2014 CIA Diversity in Leadership study commissioned by the Director of the CIA, one of the nation highest intelligence and security agency cited that the lack of diversity in its leadership ranks is of great concern as diversity is "critical to the mission". The agency further stated that "a lack of diversity of thought and experience was identified by congressional committees and independent commissions as a contributing to past intelligence failures…that diversity is mission critical is no longer a debatable proposition – if it ever was"

The Shortages in the Cybersecurity Workforce Diversity

According to Frost & Sullivan's 2017 International Information Systems Security Certification Consortium (ISC) 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 2014 – 2060.

In a recent USEOC Report, projections for selected STEM occupations with fast employment growth, projected 2012-22, Information Security Analysts have a 37% projected growth rate (currently 75,100 jobs annually and 102,500 jobs created annually by 2022), with a Median Annual Wage in 2013 of $88,590.00. Global Information Security Workforce Sub-Reports issued by various industry groups (to include (ISC)2) cite the consistent underrepresentation of African Americans and Hispanics in STEM careers. Only some 6% of STEM workers are African American compared to an overall 10% of the U.S. workforce. Similarly, Hispanics comprise only 7% of the STEM workforce while making up 15% of the U.S. workforce. In the past, human bias was understood to be largely a conscious and intentional reason for such gross underrepresentation. New research from the fields of neuroscience and sociology now suggest that human biases are largely unconscious and unintentional.

As the demographics of the U.S. population continue to become more diversified, the importance of increasing the participation of women and minorities in the workforce becomes of paramount concern. Ashley Tolbert, a recent Information Security graduate from Carnegie Mellon now working in the Bay Area in Cyber Security Operations, writes of her experiences as a student, intern and professional in the cybersecurity field that “a lack of diversity and inclusion in the information security field is one of the foremost impediments to attracting and retaining diverse talent, which the industry sorely needs. Since cybersecurity is one of the biggest challenges to our Nation’s national and economic security and we’re facing a major talent shortfall in the industry, strategies to ensure all capable talent regardless of race, ethnicity or sexual orientation feel welcome and included is important.”

This workforce shortfall should be of much consternation given that cybercrime and information theft, to include cyber espionage, remain the most serious economic and national security challenges that our country faces. It has also been reported that this 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 issue of digital diversity and equality, but it threatens our global economic viability as a nation.

The Roots of the Cybersecurity Workforce Diversity Goes Back to 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.

Chairman Ratcliffe, our STEM imperative cannot be more urgent for minority students 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 and Private Enterprises

Nonprofits and educations institutions are tackling the cyber 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 toward fostering the career growth of junior and mid-level practitioners into becoming the next generation of executive decision-makers. Studies by various groups, have underscored the importance of work-based learning programs, mentorship, apprenticeship, sponsorship and employee affinity groups as key strategic components of successful diversity and inclusion programs and employee retention initiatives.

Toward fulfilling these five key organizational objectives, last year ICMCP was able to accomplish the following thanks to the generosity of our sponsors,

- Awarded 10 Academic Scholarships @$5K
- Awarded 5 Certification (average $3K)
- Awarded 1 Executive Development ($16K)
- Placed 12 interns in cybersecurity positions
- Matched 17 Protégés to Mutually Matched Mentors
- Assisted and facilitated the job placements of over one 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 already accomplished the following:

- Awarded over $100K in academic scholarships
- Awarded at least 10 certification vouchers (ISC2, CompTIA, SANS, ISACA, IAPP)
- Coordinated the placement of 15 interns and 20 job-seekers

We should also mention our participation in note-worthy and government-led initiatives 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 cybersecurity and 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. NSF

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 be filling these jobs with diverse candidates.

Diversity Wins

Chairman Ratcliffe, several studies have proven that diverse teams wins 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, who 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

Mr. Chairman, in closing, there are lots of vital efforts underway to tackle the problem we have titled the “The Great Diversity Divide” and progress is being made. Sadly however, with over 250, 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, same with 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 before you today, and I look forward to any questions that you have.