STATEMENT FOR THE RECORD OF

AMELIA ESTWICK, PHD, DIRECTOR, NATIONAL CYBERSECURITY INSTITUTE AT EXCELSIOR COLLEGE, FACULTY PROGRAM DIRECTOR, SCHOOL OF GRADUATE STUDIES, MASTER OF SCIENCE IN CYBERSECURITY PROGRAM

BEFORE THE U.S. HOUSE OF REPRESENTATIVES HOMELAND SECURITY SUBCOMMITTEE ON

CYBERSECURITY, INFRASTRUCTURE PROTECTION AND INNOVATION

"GROWING AND DIVERSIFYING THE CYBER TALENT PIPELINE"

May 21, 2019, 2:00 PM | 310 Cannon House Office Building

Thank you, Chairman Thompson, Ranking Member Rogers, and Members of the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Innovation. I am proud and honored to appear before you today to discuss the challenges for growing and diversifying the cyber talent pipeline. According to the 2018 (ISC)2 Cybersecurity Workforce Study, the shortage of cybersecurity professionals is close to 3 million worldwide, with a shortfall of approximately 500,000 in North America. In addition, the report states "*63% of respondents report that their organizations have a shortage of IT staff dedicated to cybersecurity while 59% say their companies are at moderate or extreme risk of cybersecurity attacks due to this shortage."* Technology has become ubiquitous and necessary for conducting every facet of our daily lives; however, with the ever-present host of cyberthreats our nation is facing, it is imperative we have a workforce that is skilled and educated to address cyberthreats as well as our future technological needs.

My name is Dr. Amelia Estwick, director of the National Cybersecurity Institute (NCI) at Excelsior College and faculty program director for the Excelsior College School of Graduate Studies' Master of Science in Cybersecurity Program. Prior to my academic position, I spent more than 20 years in government service within the intelligence community (National Security Agency) and Uniformed Services (United States Army). I was the first African-American woman to graduate from NSA's Computer Network Operations Development Program, which was a three-year intense cyber operations technical leadership program focused on all aspects of cyber operations to include: attack, exploitation, and defense. At NSA, I held multiple technical leadership positions, including computer science researcher and senior cybersecurity analyst, and prior to my departure in 2016, I was one of the few women technical directors within NSA's Cyber Threat Operations Center; a 24/7/365 cyber operations center responsible for monitoring and defending Department of Defense (DoD) networks globally. For me, reaching the technical director position was a great achievement, considering research by (ISC)2 show that while "*minority representation within the cybersecurity field is slightly higher (26%) than the overall U.S. minority workforce (21%)...racial and ethnic minorities tend to hold non-managerial positions, and pay discrepancies [prevail], especially for minority women.*" Although I've had a rewarding government career, my concern for the lack of diversity amongst the cybersecurity

workforce ultimately drove me to leave government service and join academia to help with the nation's need to grow and diversify the cybersecurity talent pipeline.

In 2013, I joined Excelsior College as an instructional faculty member and subject matter expert for their graduate cybersecurity courses. In 2016, I decided to join the College full-time as the NCI director and cybersecurity thought leader because I believed in its mission to provide educational opportunities to adult learners through their online programs who live across the United States and internationally. This call to service rang especially close to my heart as a veteran and knowing how important it is to provide educational services to active military members who may be stationed in remote locations. In 2014, NCI was established as an academic, training, and research center dedicated to assisting government, industry, military, and academic sectors meet the challenges in cybersecurity policy, technology and education. In addition, as part of its continuous efforts to build the cybersecurity workforce and influence an informed leadership base that implements cutting-edge cybersecurity policy, NCI launched its Initiative for Women in Cybersecurity (NCI's IWICS). As the director of NCI, I have been instrumental in collaborating with organizations, such as Women in Cybersecurity (WiCyS) and the International Consortium of Minority Cybersecurity Professionals (ICMCP) to promote activities focused on recruiting, retaining, and advancing women and minorities in cybersecurity.

Cybersecurity Across the Academic Curriculum

In March 2018, the Journal of The Colloquium for Information System Security Education (CISSE) published an article "What Constitutes Core in a Cyber Security Curriculum?" which discussed how expansive the cybersecurity field is and stressed the importance of academic institutions taking a multidisciplinary approach to teaching cybersecurity concepts. Cybersecurity curricula was originally rooted in computer science and technology programs; however, the operationalization of cybersecurity in our digital society has necessitated the expansion of a multidisciplinary curricula throughout the academic landscape. This expansion has impacted all disciplines to include business, law, health, and finance.

Cybersecurity's multidisciplinary approach is further supported by the National Information Assurance (IA) Education and Training Programs (NIETP), which manages the National Centers of Academic Excellence (CAE) programs designated by NSA and the Department of Homeland Security (DHS). The goal of the CAE program is "*to reduce vulnerability in our national information infrastructure by promoting higher education and research in Cyber Defense (CD) and to produce a growing number of professionals with expertise in CD disciplines"*. U.S. academic institutions whose cybersecurity programs meet the rigorous criteria to be either a CAE in Cybersecurity Defense Education (CDE), Cyber Operations (CO), or Research (R) are given this designation for a specified amount of years (usually five years) and an institution must apply for redesignation before it expires. Institutions with the CAE designation serve as national models for capacity-building of information security programs in higher education, while at the same time strengthening the nation's infrastructure. CAE-designated institutions benefit from internal and external recognition for faculty and graduates, collaboration opportunities with other

CAE-designated institutions, and funding from federal, state, and local organizations. According to the National Centers of Academic Excellence, more than 230 institutions have been granted the CAE-CDE designation, including Excelsior College which was designated as a CAE-CDE in 2014 (and subsequently redesignated in 2019).

Furthermore, a multidisciplinary approach helps to address the recent Executive Order on America's Cybersecurity Workforce, which proposed an *establishment of a cybersecurity rotational assignment program, to serve as a mechanism for knowledge transfer and a development program for cybersecurity practitioners*. Providing educational opportunities along with the rotational assignment program will encourage upskilling/reskilling the current federal and non-federal workforce to meet the demands of the 21st century.

The Importance of Partnering with Community Colleges

According to the American Association of Community Colleges' January 2019 report, students enrolled for credit were 56% women and 38% Hispanic/black. Comparing this to the current demographic statistic from a 2019 (ISC)2 Cybersecurity Workforce Study on Women on Cybersecurity, women make up 24% of the cybersecurity workforce; therefore, partnering with community colleges to create a cybersecurity career pathway could help to diversify the cyber talent pipeline.

There are great benefits to partnerships between community colleges and four-year colleges that offer online education. Associate degrees are often great pathways to entry-level employment. Working adults can then often leverage their compensation from work and tuition assistance benefits from employers to further their education, and online models provide the flexibility required to continue education while working. Excelsior College partners with more than 100 community colleges across the United States with 26 of these partners designated as a Center of Academic Excellence for two-year programs (CAE2Y). Excelsior works with community colleges to evaluate their programs for transfer credit into our Bachelor of Science in Cybersecurity program and help fill the growing need of cyber professionals. In addition, Excelsior provides peer mentoring for community colleges that are working to become a CAE.

Fostering Public/Private Partnerships

In 2014, the Office of Personnel Management created the Federal Academic Alliance (FAA) to provide higher education opportunities to the federal workforce at reduced tuition rates to address the government-wide skills gap needs, including the shortages in cybersecurity. Today, OPM endorses 15 colleges and universities, and focuses on providing tuition support to federal employees, and in many case, their partners and adult children.

With the endorsement of the Chief Human Capital Officers (CHCO) Council, OPM began leading this effort to:

1. Address current federal-wide and agency-specific skills gaps

2. Support career development for federal employees
3. Provide greater opportunities for federal employees to obtain college degrees, certificates, and/or college credits
4. Provide this opportunity with colleges and universities that offer an online component to address our worldwide workforce
5. Provide current college students with a greater understanding of the federal government

Colleges and universities that make up the FAA, such as Excelsior College, are vetted by OPM to ensure they meet mission critical occupational needs; are in good standing; are not-for-profit; and are regionally accredited. Most FAA member institutions offer cybersecurity and/or information technology certificates and degrees (undergraduate and graduate) to help fill federal skill gaps. Providing the additional option for certifications helps to support talent development and career advancement opportunities.

Educating Students to Prepare and Protect Our National Critical Infrastructures

The number of cyber-attacks targeting our nation's critical infrastructures are on the rise. Specifically, in 2013, 59 percent of the attacks against our critical infrastructure were reported in the energy sector (ICS-CERT, 2013). A skilled and educated workforce is an essential component in improving the security posture of our critical infrastructure. The security program of the nuclear sector is regulated by the federal government with governance under the U.S Nuclear Regulatory Commission (NRC). In addition to being competent in cybersecurity, professionals working in the nuclear and energy industries need to be aware of specific standards, requirements, and unique cyber threats.

Excelsior College has a long history of meeting the educational needs of the nuclear workforce through innovative educational solutions. In 2014, a degree program was created to address cyber security challenges facing the nuclear industry. Cybersecurity professionals in the nuclear sector require a broad range of technical skills; however, few college programs currently exist at the baccalaureate level to assure that these professionals have the unique skill sets and knowledge domains needed to protect facilities and our national security. Additionally, the critical and practical nature of nuclear and energy sectors calls for enhanced simulation-based learning to be developed. Due to Excelsior's innovative program, in June 2018, Excelsior College received a Department of Energy Nuclear Energy University Programs (DOE-NEUP) grant to purchase a web-based pressurized water reactor simulator for use in the nuclear engineering technology program. The **~$250K grant** provides funding to:

- support plant simulation to enhance student achievement of higher cognitive learning outcomes through "learning by doing,"
- provide the ability to evaluate and analyze technical information during "dynamic" situations
- enhance our student's experiential learning activities, and by doing so, enhance the student's ability to meet industry needs
- enable students to advance their understanding of key theories and concepts in the nuclear technology field to better protect against cyber threats

The value of government funding to support the development of these lab-based activities means without such support, higher education institutions might not be able to adopt this important technology. Therefore, there is an increasing need to expand government funding of experiential learning, especially in an online environment, where skills shortages in cybersecurity can only be filled by shifting people from one industry/occupation to cybersecurity fields.

Excelsior works closely with RCNET (Regional Center for Nuclear Education and Training) to partner community colleges and corporations to further advance the integration of cybersecurity measures within the energy field with the support of the National Science Foundation's Advanced Technological Education (ATE) program. These programs implemented at the College directly address the President's Executive Order (EO) 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure as well as EO on America's Cybersecurity Workforce to identify and evaluate skills gaps for federal and non-federal cybersecurity personnel with an emphasis on protecting our nation's critical infrastructures.

Addressing K–12 Cybersecurity Education

According to Education Superhighway's 2018 State of the States report, "*40.7 million more students have high-speed broadband in their classrooms*." With more than 44 million students connected to the Internet since 2013, this means "*98% of school districts can take advantage of digital learning*." This is an impressive number for schools that can provide digital learning for their students in addition to integrating technology into the classroom as schools become increasingly reliant on technology and sophisticated IT systems for teaching, learning, and school operations. If you consider millions of mobile PCs (such as notebooks/Macs, netbooks, tablets, and Chromebooks) are being purchased by U.S. K–12 schools every year, think about the challenges these schools face trying to secure this infrastructure against cyber threats; a daunting prospect for any school district to counter. Programs to educate the K–12 ecosystem are important not only because there's a need to protect these resources, but also this demographic represents the next generation of cybersecurity professionals.

One program addressing the K–12 population is the NSA/National Science Foundation (NSF) GenCyber Program. The GenCyber program provides summer cybersecurity camp experiences for students and teachers at the K–12 level. "*The goals of the program are to increase interest in cybersecurity careers and diversity in the cybersecurity workforce of the nation, help all students understand correct and safe online behavior and how they can be good digital citizens, and improve teaching methods for delivery of cybersecurity content in K–12 curricula. GenCyber is providing a solution to the nation's shortfall of skilled cybersecurity professionals by ensuring that enough young people are inspired to direct their talents in this area, which is critical to the future of our country's national and economic security as we become even more reliant on cyber-based technology in every aspect of our daily lives*."

In 2018, Excelsior College partnered with two Boards of Cooperative Education Services (BOCES) serving 46 districts with a combined population of more than 80,000 students throughout New York State's Capital Region to offer one teacher camp for middle and high school educators. The GenCyber **~$100K** grant provided Excelsior College and BOCES an opportunity to offer the first GenCyber cybersecurity camp in the New York State Capital Region. The camp taught 30 middle and high school educators from different disciplines and

diverse populations about foundational cybersecurity concepts. GenCyber programs support the President's EO on America's Cybersecurity Workforce on developing and implementing educational programs for K–12 which is proposing to reward an annual Presidential Cybersecurity Education Award to elementary and secondary school educators who best instill skills, knowledge, and passion with respect to cybersecurity and cybersecurity-related subjects.

Expanding Opportunities for Experiential Learning

One of the keys to cybersecurity education is ensuring students are prepared upon graduation with practical, hands-on skills. Employers need employees with competencies that are directly related to the threats they encounter within their organizations. Opportunities for experiential learning allows the student to not only gain real-world experiences but also the ability to reflect on those experiences and build on their knowledge is important for reskilling/upskilling cybersecurity professionals. Some examples of experiential learning are:

Cyber Competitions/Capture-the-Flag (CTFs)/Cyber Ranges

Cyber competitions originated from cyber defense exercises that were traditionally designed by the U.S. military service. Over the years, cyber competitions or CTFs have become increasingly popular for students to partake in to assess their competencies and skills. The challenges are designed to replicate the type of threats that are prevalent in the workplace and participants compete with other college teams to identify and capture flags within the exercises. Besides the hands-on experiences, students benefit from each other in acquiring the soft skills that are sometimes lacking in the technical arena, such as: teamwork, leadership, communication, and problem solving which are all crucial skills to have in cybersecurity. The President's EO on America's Cybersecurity Workforce supports a plan to develop "*an annual cybersecurity competition (President's Cup Cybersecurity Competition) for Federal civilian and military employees. The goal of the competition shall be to identify, challenge, and reward the United States Government's best cybersecurity practitioners and teams across offensive and defensive cybersecurity disciplines."* NCI, through our student chapter of the National Cybersecurity Student Association (NCSA), has sponsored Excelsior students for the past four years to compete in cyber competitions; which resulted in several of our teams placing among the top 100 national teams.

Apprenticeships/Internships/Work-Study

While colleges and universities can and do infuse lab simulations, tabletop exercises, and case studies within their courses, internships (both virtual and in-person) provide opportunities for students to work within the contexts of the real world. As part of these programs, they can get firsthand experience with the issues facing business, government, and nonprofits. This is particularly important for individuals looking to change their career to take advantage of opportunities in cybersecurity. At Excelsior College, we have worked on developing an option for students to complete an internship for credit. By participating in internships, students gain practical work experience that they can use to demonstrate their skills and potential to future employers. For employers hosting interns, there is a potential to increase capacity in the short term and build talent pipelines in the long run. The internship course at Excelsior College is a 15-

week instructor-led course that runs simultaneous to the internship experience. Students are expected to spend 9 hours per week on their internship experience and work activities and write a weekly reflective journal about the applicability of the experience to their degree program and future career plans.

Conclusion

Mr. Chairman, in closing, there are several efforts that support growing and diversifying the cyber talent pipeline; however, we must be mindful of how those programs are executed to ensure equitable representation of women and minorities in the cybersecurity profession. As stated by Rick Ledgett, former deputy director of the National Security Agency, "*Getting more women and minorities into that cyber security workforce will be the key to addressing the current and expected labor shortfalls*."

With a shortfall of approximately 500,000 North America-based cybersecurity jobs, as a society we should be using all resources at our disposal to provide career pathways to ensure these jobs are filled. For me, it starts with early education at the K-12 level where education can help protect key resources and we are able to build competencies in the next generation of cybersecurity professionals. It continues with partnerships across multiple sectors, where organizations can work together to expand the workforce. And it works best when we have identified the key competencies and skills required to protect our critical infrastructures specifically and our national security generally.

Thank you for the opportunity to testify before you and the subcommittee, and I look forward to any questions you may have.