Dr. Stephen A. Cambone
Texas A&M University System
U.S. House of Representatives
Subcommittee on Cybersecurity and Infrastructure Protection
of the Committee on Homeland Security
Subcommittee on Higher Education and Workforce Development
of the Committee on Education and the Workforce
"Public-Private Solutions to Educating a Cyber Workforce"
210 House Visitors Center
Tuesday, October 24, 2017 2:30 p.m.

Introduction

Chairman Racliffe, Chairman Guthrie, Members of the Subcommittees, thank you for the opportunity to testify before you today.

I come before you this afternoon to discuss cyber security workforce development, as the recently appointed Associate Vice Chancellor for Cyber Security Initiatives for Texas A&M University System.

The System's flagship university, Texas A&M, is a land grant university. As such it is particularly attuned to meeting the workforce needs of the state and nation.

My charge is to assist in the development of a multidisciplinary program in cyber security across the 11 universities and seven state agencies that comprise the System. I have been asked to engage leaders across the state and nation, both in the public and private sector, to identify the most pressing needs and then look to the resources of the System to determine whether and in what way we can contribute to meeting those needs.

Our objective is to develop transformational cybersecurity capabilities, implemented by a well-educated and trained workforce, that support the United States' mission of protecting against and combatting large-scale cyberattacks.

I come to the Texas A&M System after a career in both the public and private sector. During my time in the Pentagon as senior official from 2001-2006, I was witness to and occasionally helpful in advancing the national interest and capabilities in the cyber domain. While serving as the first Undersecretary of Defense, I had oversight of on behalf of the Secretary of a variety of cyber issues.

My subsequent experience in the private sector included responsibility for a substantial business unit that supported several government customers with interests in the cyber domain. That business unit also explored as early as 2008 the use of commercial communications and devices—and their attendant security—to manage small robots and handheld drones, controlled through cellular networks and reporting to the user on wearable devices, for a wide variety of applications.

Given our increasing reliance on cyber-physical systems—the power grid and the Internet of Things being two examples – there is a compelling need for well educated professionals to address the cybersecurity needs of the nation.

Those needs are felt at the local, tribal, state and federal level. Some put the need at more than 200,000 professionals, not including the primary, secondary or university educators.

Universities across the nation are experimenting with a variety of undergraduate and graduate degrees and professional education programs to meet the demand.

The difficulty faced in meeting the demand is both the shortage of well-educated instructors and the increasing velocity of change in the field of cybersecurity.

Within the Texas A&M University System we are addressing both issues.

Background on The Texas A&M University System Workforce Activities

The Texas A&M College of Engineering is one of the largest in the nation with over 19,000 students and numerous tenure track and professional faculty conducting research and collaborating outside of Engineering on a range of cyber-related topics.

The quality of their work, and the education it supports, has resulted in Texas A&M's designation by the NSA/DHS as a National Center of Excellence in three distinct areas: Cyber Operations, Cyber Defense Education, and Cyber Defense Research.

Texas A&M University is one of only eight universities in the US, and is the only public university in the American Association of Universities, with all three designations.

Texas A&M has created a cybersecurity minor field of study. First implemented in 2016, it is already the largest minor in the College of Engineering.

Over 300 students in six different university colleges/schools have enrolled, including 39 who have already graduated.

In the spring of 2018, the University will enroll its first cohort of students in a distinctive Masters of Engineering in Cybersecurity.

In addition, the Texas A&M Engineering Extension Service (TEEX), and the Texas A&M Engineering Experiment Station (TEES), two state agencies which are a part of the Texas A&M University System, have extensive programs in applied research and emergency response workforce development related to cybersecurity.

TEEX is a leading member of the National Domestic Preparedness Consortium and the National Cybersecurity Preparedness Consortium. Both consortia are critical preparedness partners of DHS/FEMA. Its Cyber Readiness Center provides technical assistance to private and public organizations with the intent of improving the health and security of their digital operations. It delivers, at no cost, DHS/FEMA cybersecurity courses. It provides preparatory classes for professional certifications in cyber security and provides technical assistance to prepare for cyber events. And, it conducts response exercises to prepared communities and their officials to take swift, targeted action to address an attack and limit losses.

TEES, through its EDGE program for professional and continuing education, supports the deployment of face-to-face, online and blended classes. All of its courses can be made portable. In addition, it has developed the means of providing similar services for academic instruction, enabling coursework to be presented throughout the Texas A&M University System. These assets are being woven into the cyber security initiatives sponsored by the Vice Chancellor's office.

As impressive and effective as these measures and similar efforts made in states across the nation may be, they are not sufficient to meet the increasing need for a well-educated cybersecurity workforce.

Recommendations

With your permission, I'd like to offer two suggestions that might improve the rate at which we educate and increase the cyber workforce.

Expand existing information sharing programs to meet workforce needs

DHS might select and invite researchers and educators to affiliate with each existing ISAC and ISAO, expanding the collaborative benefits of these public-private partnerships to include cyber workforce development.

Participants from higher education would be exposed to and able to conduct basic and applied research into each sector's immediate challenges. This research can benefit each sector and might be shared across sectors while simultaneously providing material for real-time updates of course curriculum. This practical knowledge could help our graduates entering the workforce to be "job ready on Day 1".

Create a Cyber Grant program to meet workforce needs

The Morrill Act recognized that the classical education then offered by institutions of higher learning were not meeting the pressing needs of the nation. It gave rise to the great land grant universities in the US. More recently, Congress created Sea and Space Grant programs to conduct research and extend the benefits of that education to local populations.

Considering the challenges we face in developing and maintaining the cybersecurity workforce, the creation of a Cyber Grant Program modeled after the three previous grant programs can be established to realize similar benefits.

It can facilitate significant advancement of cybersecurity research, education, and outreach across a broad front, including the development and delivery of portable course content that addresses all sixteen critical infrastructure sectors designated by DHS, and can be used by industry in professional development.

Conclusion

It will take time to build the cyber workforce we require. We need to be intentional and aggressive in our efforts now to yield essential returns in the future. Time is of the essence and the Texas A&M University System is ready to serve.