DEPARTMENT OF COMMERCE
National Institute of Standards and Technology

[Docket Number 170627596–7596–01]

Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development

Comments of AT&T Services, Inc.

Introduction

AT&T appreciates the opportunity to respond to NIST's Request for Information concerning cybersecurity workforce development. The extreme shortage of talent in the cybersecurity field is a national problem, and how best to address that shortage has become a topic of urgency among the government, industry and academia. Executive Order 13800 underscored the importance of this mission, making it the policy of the United States "to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace."

AT&T is an industry leader in cybersecurity, both in protecting our own network and in providing security solutions to our customers. Nevertheless, like many companies, we have experienced the effects of the national cybersecurity workforce shortage first hand. To deal with the problem, we have implemented measures designed to grow the emerging workforce, and to strengthen the company's existing workforce. AT&T approaches the cybersecurity workforce issue in a multi-faceted manner, including extensive participation in sector and cross-sector efforts surrounding cybersecurity workforce growth and development and in internal initiatives targeting all levels of the workforce. We describe a number of those initiatives below in order to help inform NIST's critical work in this area.

External Efforts/CSRIC

AT&T participated in the Communications Security, Reliability and Interoperability (CSRIC) V's Working Group 7, which was chartered to provide recommendations for the CSRIC's consideration regarding any actions the Federal Communications Commission (FCC) should take to promote improvements in cybersecurity workforce development. The Working Group specifically studied steps to enhance the transparency, skill validation, and best practices relating to recruitment, training, retention, and job mobility of personnel within the cybersecurity field.

In its final report, which was issued earlier this year, Working Group 7: 1) analyzed the application of the National Cybersecurity Workforce Framework (NCWF) to the common and specialized work roles within the communications sector; 2) identified gaps or improvements in the NCWF for evolving work roles or skill sets that should be included in sector members' workforce planning; and 3) identified, developed, and recommended best practices and implementation thereof to mitigate insider threats, including through scalable means to enhance transparency, accountability and validation of skills, knowledge and abilities within the communications sector and particularly with respect to personnel having access to the most critical elements of the nation's communications network assets. The final report also included a comprehensive list of recommendations that the communications sector continues to pursue that includes bolstering partnerships between government, academia and industry to expand curriculum and broaden opportunities for the developing cybersecurity workforce pipeline.

AT&T's Internal Efforts to Address the Cybersecurity Workforce Issue

AT&T is taking a balanced, holistic approach to cyber workforce development that invests in programs geared at younger students, cultivates the emerging workforce through curriculum development with colleges and universities, and trains or re-trains our existing workforce. Below we highlight a few of our efforts in this area.

Investment in Cybersecurity Development Programs

AT&T supports numerous efforts to cultivate a deep and diverse talent pipeline for AT&T and America. AT&T funds and supports many different programs and events that engage the workforce at younger ages, including Girls Who Code, hack-a-thons and local programs designed to foster interest in STEM careers generally, and cybersecurity careers specifically. Recently, for example, we teamed up with several organizations that help students learn and maintain STEM skills year round. One such program is All Star Code, which prepares young men of color for tech careers by providing mentorship, industry exposure and training in Computer Science. Their flagship program, the Summer Intensive, is a free 6-week program that provides real-world experiences at top tech companies, and hands-on, project-based learning. Participants finish the program with both coding skills and an entrepreneurial mindset.

Our programs also aim at promoting gender diversity in the cybersecurity field. We support Black Girls Code**,** whose chapters provide year-long programs in technology and computer science for underrepresented girls. AT&T also hosted Girls Who Code's Summer Immersion Program, a free 7-week program that teaches 10th and 11th grade girls coding, and exposes young women to tech jobs. This is our 5th year supporting the program. We also continue to support Girls Who Code alumni by actively sharing internship and full-time opportunities with girls who have participated in summer or club programs.

All of these programs are designed to spark interest in the tomorrow's workforce and to help students learn STEM skills and ultimately to strengthen the pipeline of talent feeding

American companies. Importantly, these programs do not simply support AT&T's cyber workforce pipeline, but benefit the national cyber ecosystem.

Recruiting at Universities

The AT&T College Recruiting team recruits at top schools throughout the nation. We aim to identify and attract elite cybersecurity talent at more than 300 top universities through live program overview webcasts and virtual information sessions. These efforts have resulted our ability to attract cyber talent from schools with leading cybersecurity-related programs across the nation, such as the University of Georgia, Georgia Tech, University of Maryland, the University of Texas-San Antonio, Southern Methodist University, and the University of California-Berkeley.

AT&T's Cybersecurity Development Program is designed to offer participants diverse perspectives, ideas and collaboration as they gain well-rounded knowledge in Cybersecurity.   This dynamic program consists of professional development, specialized learning curriculum, project and team leadership opportunities, and a path towards breaking new ground as we evolve our business and stay at the forefront of the Cybersecurity industry.   Through this program, we have recruited new hires for positions in a number of important roles around the country.

AT&T continues to monitor new programs dedicated to cybersecurity degrees as those programs mature. Additionally, we are broadening efforts to recruit STEM degree graduates from universities in specific areas, including cybersecurity, into internal programs that will rotate new hires through several cybersecurity roles during their first years with the company. These efforts not only permit AT&T to evaluate the cyber talent pool, but also expose these new hires to the best long term cybersecurity positions within the company.

Continuing Education for Our Workforce

AT&T takes great pride in the skill and professionalism of our employees, and we are an undisputed leader when it comes to giving them opportunities to continue to learn and grow their skills. That is particularly true in the area of cybersecurity. As the company evolves, we're making efforts to assist our existing talented workforce evolve with us. We launched our Workforce Skills Pivot Program in 2014 to offer employees the training and experience they need to be competitive. Security education is a core component of this effort.

The number of major recent cyber-attacks and the implications of these attacks underscore the need for bright, educated minds in information security. Recognizing that our workforce must become more proficient in software development and security, we incorporated training courses emphasizing security architecture principles, secure coding practices, code scanning, API security, and more. These "nanodegrees" take about 4-9 months to complete, and the aggressive and comprehensive curriculum teaches valuable skills employees can apply in real situations immediately.

For example, as part of the larger ongoing workforce transformation initiative we offer our employees the opportunity to obtain a certification in cybersecurity through a partnership program with a U.S. college's extensive cybersecurity program. The program offers a cybersecurity certificate to our employees following completion of several progressively built courses including:

- The foundations of cybersecurity
- Network security
- Mobile security
- Emerging threats and defenses
- Ethical hacking
- Policy analysis and implementation

As a practical matter, we have found that data scientists with security knowledge are among the more difficult skills to find. When necessary, we have paired a pure data scientist with a security analyst to compensate for a shortage in individuals who have expertise in both areas. In order to better fill this need in the future, we have the following programs a variety of major colleges and universities, including those that participate in Department of Homeland Security and National Security Agency's jointly sponsored National Centers of Academic Excellence Cyber Defense Program, designed to train and re-train employees in particular fields to broaden their skill into another:

- A certification in Data Science through an online education resource.
- Online Master of Science in Data Science and Analytics through a university.
- A Hybrid Online Master of Science in Data Science from through a partnership with a university.
- As one offering in a broader nanodegree program, we also offers a Nanodegree in Data Analysis.

Though our internal education program, we offer many cybersecurity training courses and established a badging program to encourage employees to further develop their skills. We also offer industry standard training and fund industry certification testing through third parties.

For example, in 2016 we provided funding for dozens of employees to take Certified Information Systems Security Professional (CISSP) training and the corresponding certification exam through a third party. We also provided funding for 150 employees to take one of three different GIAC training programs and the corresponding Global Information Assurance Certification (GIAC) certification exam through a third party. The training classes we funded lead to the following certifications:

- GIAC Information Security Fundamentals (GISF)

- GIAC Security Essentials Certification (GSEC)
- GIAC Certified Enterprise Defender (GCED)

Conclusion

Cybersecurity threats are constantly evolving, and the nation's workforce must develop and evolve the skill sets necessary to meet and defeat those threats. AT&T is heavily engaged in efforts to grow the cybersecurity workforce pipeline and to provide career-long training opportunities to employees. We urge NIST to consider the extensive voluntary efforts from industry in this area and to consider ways to collaborate and build upon these efforts going forward.