Before the
DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Gaithersburg, MD 20899

In the Matter of	)	
	)	
Strengthening the Cybersecurity of	)	Docket No. 170627596-7596-01
Federal Networks and Critical Infrastructure:	)	
Workforce Development	)	

COMMENTS OF T-MOBILE USA, INC.

Steve Sharkey
Drew Morin
John Hunter
T-MOBILE USA, INC.
601 Pennsylvania Avenue, NW
Washington, DC 20004
(202) 654-5900

August 2, 2017

TABLE OF CONTENTS

Before the
DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Gaithersburg, MD 20899

In the Matter of)
)
Strengthening the Cybersecurity of) Docket No. 170627596-7596-01
Federal Networks and Critical Infrastructure:)
Workforce Development)

COMMENTS OF T-MOBILE USA, INC.

T-Mobile USA, Inc. ("T-Mobile")[1] is pleased to respond to the Request for Information ("RFI") concerning cybersecurity workforce development.[2]

INTRODUCTION

The issues raised by the Request for Information ("RFI") and the Executive Order underlying it are timely and urgent.[3] The cybersecurity workforce gap is a well-known, global problem, which will only grow absent concerted and collaborative action between industry, academia, and government. Cybersecurity professionals have unique skills and are vital to our nation's security, but they are in perilously short supply. Because the demand for this talent currently exceeds that supply, competition for these professionals is fierce, and training and education to grow this workforce is essential. The need to focus on cybersecurity training will grow with the emergence of 5G, which will drive both the

[1] T-Mobile USA, Inc. is a wholly-owned subsidiary of T-Mobile US, Inc., a publicly traded company.

[2] Department of Commerce, National Institute for Standards and Technology, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development*, Docket Number 170627596-7596-01, Request for Information, 82 Fed. Reg. 32,172 (July 12, 2017) ("RFI").

[3] Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, 82 Fed. Reg. 22391 (May 11, 2017).

number of connected devices and the number of jobs, with cybersecurity workforce growth occurring across all industry sectors. While 5G will drive numerous customer benefits, it also risks expanding the cybersecurity workforce gap.

T-Mobile welcomes this opportunity to provide additional information regarding this critical issue. As a leading network owner and provider of nationwide wireless voice, text, and data services to nearly 70 million subscribers,[4] T-Mobile necessarily must prioritize cybersecurity in its operations and in its provision of services to customers. T-Mobile thus has a vested interest in improving cybersecurity workforce training.

T-Mobile's industry leadership in this area is reflected by the fact that its representatives co-chaired Working Group 7 ("Cybersecurity Workforce") of the fifth Communications Security, Reliability, and Interoperability Council ("CSRIC V").[5] The Federal Communications Commission ("FCC") tasked CSRIC V Working Group 7 with examining and developing recommendations regarding actions the FCC could take to enhance the transparency, skill validation, and best practices relating to recruitment, training, retention, and job mobility of personnel within the cybersecurity field, all with the overarching goal of improving the security of the nation's critical communications infrastructure. Working Group 7's efforts culminated in its March 2017 report on

[4] *T-Mobile Delivers Record Results in Q2 2017, Un-carrier Performing at Peak Levels Across the Board*, July 19, 2017, https://newsroom.t-mobile.com/news-and-blogs/q2-2017-earnings.htm.

[5] CSRIC is an advisory committee consisting largely of private sector representatives that is convened by the FCC every two years in order to provide recommendations to ensure, among other things, optimal security and reliability of communications systems.

cybersecurity workforce development.[6] Working Group 7's diverse membership included network operators, service providers, manufacturers, state and federal government, and academics,[7] and its collaboration offers NIST significant momentum for this inquiry. In fact, as discussed below, NIST has a unique opportunity to advance those recommendations through this proceeding, and T-Mobile encourages it to do so.

RESPONSES TO SPECIFIC QUESTIONS

I. GENERAL INFORMATION

1. Are you involved in cybersecurity workforce education or training? If so, in what capacity?

As noted, T-Mobile is a leading network owner and service provider and thus necessarily is engaged in cybersecurity workforce development for its own employees and for its partners in industry more broadly.

T-Mobile's "Cybersecurity Co-Op Program" illustrates its commitment to cybersecurity training and education. The program is a local pipeline of "early in career" cybersecurity specialists who have proven capability and cultural fit with T-Mobile. It includes a pilot educational partnership with the Cybersecurity Program at the University of Washington-Bothell's Center for Information Assurance and Cybersecurity ("CIAC"), which is one of a limited number of institutions designated by the National Security Agency ("NSA") as a Center for Academic Excellence in Research and in Cyber Defense Education. The CIAC serves as a resource for existing T-Mobile employees to develop

[6] CSRIC V Working Group 7, *Final Report – Cybersecurity Workforce Development Best Practices Recommendations*, Mar. 2017, https://www.fcc.gov/files/csric5-wg7-finalreport031517pdf ("CSRIC WG7 Report").

[7] *Id.* at 10 (listing membership).

skills and knowledge in the cybersecurity profession. In particular, it includes opportunities for: (1) Certified Information Systems Security Professional ("CISSP") and other industry certifications; (2) Guest Instructor/Lecturer opportunities; (3) Threat Intel & Incident Response Lab; and (4) Cybersecurity Operations Center.

In addition to the resources of the CIAC, the "Cybersecurity Co-op Program" leverages the structure and mechanisms of T-Mobile's existing "TechX Program,"[8] to include allocation of participant roles; recruiting and sourcing tools and process; hiring practices; pay rates; NDAs; onboarding; and learning and development. Students in the program work in a ten-person cohort, working half-time over the course of three quarters (nine months). They are required to complete a three-quarter Cybersecurity Certificate Program at UWB-CIAC, UW-Bothell course and degree requirements, and a project that they present to T-Mobile executives. T-Mobile has already witnessed numerous short-term and long-term benefits arising from this program for various stakeholders:

- Accelerated professionalization of students;
- Blending academia with industry;
- Development of a replicable cooperative education model;
- Government (NSA) sponsorship/scholarships benefits;
- Alignment with (telecom) industry specific needs;
- 90%+ conversion from intern to full time employee; and
- Expansion to other (non-telecom) critical infrastructure players.

[8] *See, e.g.*, T-Mobile, 2017 TechX Internship Program – Devops Track, https://tmobile.careers/job-details/engineering/73398BR-2017-techx-internship-program-devops-track-bellevue-wa.

Beyond the Cybersecurity Co-op Program, T-Mobile also participates in industrywide collaborative efforts focused on cybersecurity workforce education. In addition to CSRIC V's Working Group 7, these include:

- The Joint Task Force on Cybersecurity Education, a collaboration between international computing societies, academic institutions, industry, and government to develop comprehensive curricular guidance. (Described further below in response to Section II Question 1.)
- Internship programs and partnerships between academia and industry, to provide the bridge to the specialized skills required by industry.
- The development of the National Cybersecurity Workforce Framework ("NCWF"), which as described further below enables a common lexicon to understand and communicate workforce requirements.

II. GROWING AND SUSTAINING THE NATION'S CYBERSECURITY WORKFORCE

1. What current metrics and data exist for cybersecurity education, training, and workforce developments, and what improvements are needed in the collection, organization, and sharing of information about cybersecurity education, training, and workforce development programs?

There are already several hard estimates regarding current cybersecurity workforce gaps and future employment needs, most of which are already in the public domain. For instance, the Global Information Security Workforce Study released earlier this year projects a shortage of 1.8 million professionals by 2022, a 20 percent increase over the forecast made in 2015.[9] Symantec estimates 6 million positions globally with 1.5 million

[9] Frost & Sullivan, Center for Cyber Safety and Education, *2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk*, at 2, https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf.

cybersecurity job openings unfilled by 2019.[10] Cisco has put the global figure at one million unfilled cybersecurity job openings.[11] While these figures vary somewhat, they uniformly support the incontrovertible fact that there is a serious and growing cybersecurity workforce gap.

Due to industrywide collaboration that has already occurred, a number of valuable and effective mechanisms now exist for sharing information about cybersecurity training and education. NIST and the Department of Homeland Security ("DHS"), working collaboratively on the National Initiative for Cybersecurity Education ("NICE"), have developed a National Cybersecurity Workforce Framework ("NCWF") as a fundamental reference resource to support cybersecurity workforce development.[12] NICE continues to drive the update process for that framework.[13] T-Mobile believes that NICE should continue to encourage participation across all sectors, especially those that operate critical

[10] Steve Morgan, *One Million Cybersecurity Job Openings In 2016*, Forbes, Jan. 2, 2016 (citing projection by Symantec CEO); Symantec Cyber Career Connection, Collaborating to Build the Workforce of Tomorrow, https://www.symantec.com/about/corporate-responsibility/your-information/cyber-career-connection (citing Taylor Armerding, *Confronting the widening infosec skills gap*, CSO, May 15, 2015, http://www.csoonline.com/article/2922381/infosec-careers/confronting-the-widening-infosec-skills-gap.html).

[11] Cisco, *Mitigating the Cybersecurity Skills Shortage: Top Insights and Actions from Cisco Security Advisory Services*, at 2 & n.3 (citing *Cisco Security Capabilities Benchmark Study* (Oct. 2014)), http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf.

[12] *See, e.g.*, NIST, *NICE Cybersecurity Workforce Framework*, https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework.

[13] Comments on the most recent NCWF update were gathered through early January 2017, and a further revision is expected to be published imminently. *See id.*; *see also infra* at 9 & n.17.

infrastructure, to ensure broader awareness and enhance sharing of cybersecurity workforce development programs and frameworks.

In addition, the Association for Computing Machinery ("ACM") has partnered with the IEE Computer Society ("IEEE-CS"), the Association for Information Systems Special Interest Group on Security ("AIS SIGSEC"), and the International Federation for Information Processing Technical Committee on Information Security Education ("IFIP WG 11.8") to develop cybersecurity curricula guidelines for post-secondary degree programs. The Joint Task Force ("JTF") launched by these international computing societies recently issued and sought comments on a report setting forth proposed guidance on this subject and expects to publish a final report later this year.[14] As it typically takes years to develop this type of academic guidance, this is a key milestone in addressing the requirement for a common core curriculum for cybersecurity education. T-Mobile encourages NIST to support this cross-sector initiative to define a framework for the development of cybersecurity courses of instruction and to raise awareness of these efforts.

Another promising resource that can help ground and reinforce real-world cybersecurity understanding is hands-on experience in a "cyber lab" or "cyber range." T-Mobile is actively engaged with UW-Bothell in the development of a cyber range tailored to the unique needs of the communications sector. Other more general purpose examples of these resources include the University of Southern California (DeterLab), Syracuse University (SEEDLab), and Michigan Coalition (MeritLab). CyLab at Carnegie Mellon University is a good example of a combination of research, hands-on education and

[14] *See, e.g.*, Joint Task Force on Cybersecurity Education, https://www.csec2017.org/.

industry partnership.[15] CyLab is a National Science Foundation ("NSF") CyberTrust Center and a key partner in the NSF-funded Center for Team Research in Ubiquitous Secure Technology.

2. Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?

Understanding and agreement on these areas has grown through collaborative industry efforts like CSRIC V's Working Group 7 and the NCWF, as well as through the efforts of NICE and the JTF ACM working groups.

As Working Group 7's final report explains, the NCWF provides a blueprint to categorize, organize, and describe cybersecurity work into "Categories," "Specialty Areas," "Competencies," and Knowledge, Skills and Abilities ("KSAs"), providing a common language to speak about cyber roles and jobs and to help define personal requirements in cybersecurity.[16] Specifically:

- Categories are common major functions regardless of job titles or other occupational terms. The NCWF includes seven Categories: Securely Provision, Operate and Maintain, Collect and Operate, Analyze, Protect and Defend, Oversight and Development, and Investigate.

- Specialty Areas are common types of cybersecurity work which are grouped with similar areas under a specific Category. The NCWF defines 31 Specialty Areas.

- Competencies are areas of expertise required for the successful performance of a job function; these are defined in the framework through the association of specific KSAs. NICCS identifies 65 Competencies.

[15] Carnegie Mellon University CyLab, https://www.cylab.cmu.edu/.

[16] CSRIC WG7 Report at 8-9; *see also* National Initiative for Cybersecurity Careers and Studies, *Cybersecurity Workforce Framework*, https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework.

- KSAs are the attributes required to perform a job and are generally demonstrated through qualifying experience, education, or training experience, education, or training. Knowledge is a body of information applied directly to the performance of a function. Skill is an observable competence to perform a learned psychomotor act. Ability is competence to perform an observable behavior or a behavior that results in an observable product. The NCWF defines 369 KSAs that can be each associated with one or more Specialty Areas.

Coincident with the drafting and publication of CSRIC V Working Group 7's report, NICE released an update to the NCWF that incorporates Work Roles and Tasks.[17] These enhancements to the Framework will provide a better linkage between the KSAs and the requirements of actual job openings in the cybersecurity workforce. T-Mobile supports this addition. NIST can promote further understanding by encouraging awareness and voluntary adoption of this construct.

3. Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?

As noted, T-Mobile prioritizes cybersecurity education and training in all of its operations and has taken a leadership role within industry. T-Mobile's security and privacy policies map to industry appropriate control standards that in turn map to various control frameworks (*e.g.*, NIST's Cybersecurity Framework, Payment Card Industry Data Security Standard, etc.), enabling control effectiveness and control enforcement; T-Mobile's internal workforce training emphasizes these controls.

4. What types of knowledge or skills do employers need or value as they build their cybersecurity workforce? Are employer expectations realistic? Why or why not? Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline?

[17] Draft NIST Special Publication 800-181, *NICE Cybersecurity Workforce Framework (NCWF)*, Nov. 2016, http://csrc.nist.gov/publications/drafts/800-181/sp800_181_draft.pdf.

How do these types of knowledge and skills vary by role, industry, and sector, (e.g., energy vs financial sectors)?

Cybersecurity professionals have a wide range of unique skills. As noted above, the NCWF defines a total of 369 KSAs that each can be associated with one or more specialty areas or work roles. Employer expectations are driven by the role-specific requirements. Unfortunately, the current environment does not provide a common baseline set of skills from which to build the role specific knowledge necessary to meet employer workforce requirements. The development of cybersecurity curriculum guidelines is needed to address this gap.

Further, each sector needs to support the development of specific skills unique to their requirements. For example, T-Mobile requires technical skill related to specific network protocols, technologies, and operations that are unique to the communications sector. These skills include understanding of core network protocols such as Signaling System 7 (SS7), Diameter, Session Initiation Protocol (SIP), and Voice over LTE (VoLTE). Further, there are innovations in core technologies such as Network Function Virtualization (NFV) and Software Defined Networking (SDN). These skills are not going to be developed in the normal academic course of study and require new and innovative partnerships between industry, government and academia. CSRIC V’s Working Group 7 identified additional communications sector-specific KSAs and Specialty Areas to be added to the NCWF. This is another area where NIST and industry can benefit from encouraging broader participation in the review and submission of enhancements to the NCWF.

5. Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today? What makes those programs effective? What are the goals for these programs and how are they successful in reaching their goals? Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs?

Programs such as the T-Mobile program discussed above offer a good example of an effective training and educational opportunity that is capable of being replicated. This program is effective in large part due to its combination of industry and academic knowledge and expertise.

The CyberCorps®: Scholarship for Service ("SFS") program is an example of a successful government program.[18] By providing full scholarships in exchange for a work commitment, this program creates more opportunities for students to pursue a course of study in cybersecurity.

6. What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?

In T-Mobile's experience, several key challenges to effective cybersecurity workforce training and education persist. For one thing, curriculum guidelines are still evolving; there is no standard baseline. In addition, the skill level is not entry level; each industry requires specialization, and that translates to customized training.

Further, there is a lack of qualified instructors. Industry and government recruiting of skilled practitioners from universities has depleted the number of qualified instructors, making it more difficult to educate and develop the future workforce. Likewise, recruiting

[18] U.S. Office of Personnel Management, CyberCorps®: Scholarship for Service, https://www.sfs.opm.gov/.

from Department of Defense and other existing practitioners does not address the workforce gap; like squeezing a balloon, it merely moves it.

Finally, technology is continuing to evolve rapidly, such that education and training have difficulty keeping up with the latest advances. An approach based on an extensible framework and voluntary adoption is required to provide the flexibility to keep pace with this environment.

7. How will advances in technology (e.g., artificial intelligence, Internet of Things, etc.) or other factors affect the cybersecurity workforce needed in the future? How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems (CPS)?

5G deployment is driving unprecedented growth. Cisco and Microsoft have predicted 50 billion devices will be connected to the Internet by 2020,[19] and global spending on cybersecurity products and services is predicted to exceed $1 trillion over the next 5 years.[20] By 2020, data volumes online are expected to be 50 times greater than today.[21] These developments increase the human attack surface, which is expected to reach 4 billion people by 2020.[22]

[19] Gary Wachowicz, *Cities & Cybersecurity: Why Trust Microsoft?*, Mar. 3, 2016, https://enterprise.microsoft.com/en-au/articles/industries/citynext/digital-cities/cities-cybersecurity-why-trust-microsoft/; Dale Evans, *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, Cisco White Paper, at 3 (Apr. 2011), http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[20] Steve Morgan, *Cybersecurity Spending Outlook: $1 Trillion from 2017 to 2021*, CSO Online, June 15, 2016, http://www.csoonline.com/article/3083798/security/cybersecurity-spending-outlook-1-trillion-from-2017-to-2021.html.

[21] Microsoft Secure Blog, *The Emerging Era of Cyber Defense and Cybercrime*, Jan. 27, 2016,

This dramatic technology expansion also is expected to drive job growth – meaning more individuals requiring cybersecurity training and education. The economic benefit of 5G is estimated to be at $500 billion and result in the creation of an estimated 3 million jobs across all sectors. As our nation develops and deploys 5G technologies, it is estimated that for every job created among network providers, there could be up to 40 new jobs generated in other sectors.[23] The result is that cybersecurity job growth as a result of 5G will have a dramatic impact on all industries and government, not just the communications sector.

On the other hand, machine learning is also an evolving technology that will be found in cybersecurity products and services to support 24/7 always-on automation without manual intervention. By 2020, 10 percent of penetration tests will be conducted by machine-learning-based smart machines, up from 0 percent in 2016.[24] While these "force multiplier" technologies will result in increased productivity, the gap is still forecast to continue to grow rapidly, and the need for specialized skills is likely to continue to grow at an even faster pace.

8. What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the Nation's cybersecurity workforce, taking into account needs and trends? What steps should be taken: (i) At the Federal level? (ii) At the state or local level,

https://blogs.microsoft.com/microsoftsecure/2016/01/27/the-emerging-era-of-cyber-defense-and-cybercrime/.

[22] *Id.*

[23] Accenture Strategy, *Smart Cities: How 5G Can Help Municipalities Become Vibrant Smart Cities*, at 1 (2017), https://newsroom.accenture.com/content/1101/files/Accenture_5G-Municipalities-Become-Smart-Cities.pdf.

[24] Gartner 7 Top Security Predictions for 2017 (June 13, 2017), http://www.gartner.com/smarterwithgartner/7-top-security-predictions-for-2017/.

including school systems? (iii) By the private sector, including employers? (iv) By education and training providers?

CSRIC V Working Group 7's March 2017 report identified a number of actions that can be taken by various sectors going forward to grow and sustain the cybersecurity workforce. T-Mobile urges NIST to consider ways to promote implementation of these recommendations both in the communications sector and beyond. Indeed, NIST may now be in the best position to do so, since the newly re-chartered CSRIC no longer includes a working group dedicated to workforce issues[25] – meaning that the FCC is less likely to advance this issue than was the case when Working Group 7 undertook its efforts in 2015 through 2017. In other words, NIST can pick up where the FCC left off and build on the solid foundation created just months ago by CSRIC V's Working Group 7. The CSRIC recommendations were crafted with reference to the communications industry, but they are not specific to any one sector and could easily be generalized and applied to other industry sectors.

Per the Working Group 7 recommendations, NIST and the federal government should consider the following steps:

1. *Support a Process for the Communications Industry to Cooperatively Support Updates to the National Cybersecurity Workforce Framework.* The dataset produced by Working Group 7 in coordination with the Cybersecurity Workforce Alliance ("CWA") – the process and results of which is detailed in the working group's final

[25] CSRIC VI, Working Group Descriptions, June 23, 2017, https://www.fcc.gov/files/csric6wgdescriptions6-2017pdf.

report[26] – is not a static reference and needs to evolve as our industry workforce needs evolve. Possible options for facilitating that evolution include supporting communications industry partnerships with the CWA and encouraging participation in the NICE Working Group to influence updates to the NCWF. (The NICE Working Group is described further below.)

2. *Encourage Communications Industry Development of Cooperative Work-Study Program Partnerships.* Work-study programs assist with recruiting and serve as a tool to engage potential talent to explore cybersecurity as a career. Internship and apprenticeship programs can be homegrown or based on existing partnerships. These programs can be used to enhance recruiting efforts or hone skills of new/existing staff.

3. *Engage with the Communications Industry to Develop or Expand Scholarship for Service Programs in Industry.* This model draws on the success of the U.S. government CyberCorps program, described above. This option differs from an internship program in that the student is "paid" to pursue his/her degree and, in return, commits to work for the "provider" for a certain period of service following graduation.

4. *Encourage Communications Industry Cybersecurity Professionals to Help Train the Next Generation.* The academic community has a severe shortage of qualified cybersecurity instructors. The communications industry, partnering with the academic community, could augment the resources available to help to address this gap. The goal is to increase the volume while also providing communications industry specific content focus.

[26] CSRIC WG7 Report at 15-16.

5. *Encourage the Communications Industry to Participate in the Development of Curriculum Guidelines by the Joint Task Force on Cybersecurity Education.* Curriculum guidelines provide the basis for the academic community to deliver consistency in developing future cybersecurity programs. By supporting the JTF effort (described above), the communications industry will be able to ensure that the guidelines reflect the needs of the entire industry.

6. *Partner with Communications Industry, Public Safety, and Federal GenCyber to Develop a Cybersecurity Distance Learning Program for Public Safety and Rural Communities.* The public safety community has a unique challenge to provide cybersecurity training especially in rural areas. GenCyber is reaching out nationwide to deliver regional exposure to cybersecurity skills.[27] Distance learning in partnership with local schools, community colleges, and universities could address the need and develop new workforce sourcing opportunities.

Further, and again per the Working Group 7 recommendations, steps that industry and employers can take to grow and sustain the nation's cybersecurity workforce include:

1. *Support Innovative Cybersecurity Workforce Development Initiatives such as the CyberBlue Program to Engage Populations with Disabilities.* The cybersecurity workforce is characterized by people that think critically, recognize patterns, efficiently analyze data, discard preconceptions, and focus deeply. These characteristics are present in many of the 70 million people worldwide living with autism; by 2020, the number of

[27] *See, e.g.*, GenCyber, Inspiring the Next Generation of Cyber Stars, https://www.gen-cyber.com/; NSA, Resources for Students: GenCyber Program, https://www.nsa.gov/resources/students/summer-camps/gencyber/.

autistic adults in the U.S. is expected to exceed 3 million. CyberBlue™ is a collaboration between the George Washington University Institute for Information Infrastructure Protection and Autism and Neurological Disorders Institute to prepare autistic adults to be "cyber warriors." This represents an under-utilized resource that should be engaged as part of a nationwide solution to addressing the gap in skilled candidates. In the United Kingdom, the Government Communications Headquarters ("GCHQ"), which is responsible for signals intelligence, currently operates a successful neurodiversity program that employs more than 300 people with neurological "differences" that bring unique strengths to the workforce.[28]

2. *Communications Industry Cybersecurity Experts Should Join the NICE Working Group or One of its Subgroups.* The NICE Working Group was established to provide a mechanism by which public and private sector participants can develop concepts, design strategies, and pursue actions that advance cybersecurity education, training, and workforce development.[29] As such, it provides a vehicle to continue to influence the development of best practices for cybersecurity workforce development.

3. *The Communications Industry Can Benefit by Growing Awareness of, and Supporting Programs Encouraging, K-12 Youth to Study Cybersecurity.* Example programs such as GenCyber and the BATEC Summer Bridge program encourage early

[28] Rhiannon Lucy Cosslett, *Autism in the workplace – an opportunity not a drawback*, The Guardian, Nov. 11 2016, https://www.theguardian.com/lifeandstyle/2016/nov/11/autism-in-the-workplace-an-opportunity-not-a-drawback.

[29] National Initiative for Cybersecurity Education Working Group, https://www.nist.gov/itl/applied-cybersecurity/nice/about/working-group.

development of and interest in a cybersecurity skillset. Industry participation in internship programs, seminars, and after-school programs have the same effect. In addition, supporting “cyber as a sport” competitions would increase awareness of the opportunities in cybersecurity.

*   *   *

By endorsing the Working Group 7 recommendations (and asking that NIST do so as well), T-Mobile does not mean to suggest that these ideas should be pursued exclusively. Indeed, there may well be additional steps and programs, whether in existence already or not, that would contribute to the overarching goal of promoting cybersecurity workforce training. But the above recommendations have resulted from the very sort of collaborative process that NIST is seeking to pursue in this inquiry and thus provide an expedited path toward achieving the objectives set forth in the RFI and the underlying Executive Order 13800.

CONCLUSION

Strengthening the nation's cybersecurity workforce will be – and must be – an ongoing, collaborative initiative. T-Mobile is eager to participate in that process and to leverage the progress and lessons it has attained thus far.

Respectfully submitted,

By: __*/s/_Steve Sharkey*___________

Steve Sharkey
Drew Morin
John Hunter
T-MOBILE USA, INC.
601 Pennsylvania Ave., NW
Washington, DC 20004
(202) 654-5900

August 2, 2017