Before the Department of Commerce
National Institute of Standards and Technology
Washington, D.C.

Request for Information	)	
	)	Docket No: 160725650-6650-1
Current and Future States of	)	
Cybersecurity in the Digital Economy	)	

COMMENTS OF CTIA

Thomas C. Power
Senior Vice President and General Counsel

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John M. Marinho
Vice President, Technology and Cybersecurity

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-0081
www.ctia.org

September 9, 2016

TABLE OF CONTENTS

Page

I. Executive Summary. 1

II. The United States Has Developed Effective Cybersecurity Policy Centered On Public-Private Partnerships. 2

III. The Communications Sector Has Been Fully Engaged On Critical Infrastructure Cybersecurity And Is Leading In 5G Innovation And Security. 4

A. The Communications Sector Relies On Partnerships, Evolving Standards And Best Practices, And Information-Sharing To Meet Security Needs. 4

B. The Government Should Support Vital Partnerships and Industry Efforts. 7

IV. The Internet of Things, Powered by 5G Wireless, Will Drive The Digital Economy, And Industry Is Working Tirelessly To Ensure Its Security....8

A. As IoT Evolves, Industry Is Addressing Security. 8

B. The Government Should Resist Regulatory Impulses That Will Stymie IoT Innovation. 9

V. Public Awareness and Good Cyber Hygiene Are Critical, And Will Benefit From Industry Leadership Rather Than Mandates. 10

VI. Increasingly Global Challenges Demand U.S. Leadership On Cybersecurity Standards, Criminal Prosecutions, And Norms For State Action. 12

VII. Innovation In Identity and Access Management Will Drive Security, Through Promising Approaches Like Biometrics. 14

VIII. The Nation Faces A Scarcity of Skilled Cyber Workers, And The Communications Sector is Addressing The Challenge. 16

IX. As the Government Remains Under Attack, Federal Governance Must Improve to Protect Government Functions, Data and Trust. 17

X. In Conclusion, At This Inflection Point, Core Principles Have Emerged To Guide Federal Policy. 18

A. Public-Private Partnerships Are The Bedrock Of Cybersecurity Policy. 18

B. The Government Should Exercise Regulatory Humility. 19

C. Flexibility Is Key Because Threats And Responses Do Not Stand Still....19

D. The Government Should Promote Voluntary Standards and Technological Neutrality. 19

E. Global Threats To The Internet And Communication Network Require The United States' Leadership. 20

F. Sensitive Vulnerability Information Can Be Exploited, And Must Be Treated With Great Care. 20

G. User Education And Good Cyber Hygiene Are Critical. 21

H. The Government Must Work To Avoid Domestic and Global Fragmentation. 21

I. Executive Summary

CTIA[1] welcomes the opportunity to help the Commission on Enhancing National Cybersecurity ("Commission") refine federal cybersecurity policy as the nation confronts the next generation of communications technology.[2] In these comments, CTIA addresses challenges and opportunities in: critical infrastructure, the Internet of Things ("IoT"), public awareness, workforce, international markets, identity and access management, and federal governance.[3]

Federal cybersecurity policy has been incremental, non-regulatory, and driven by the private sector. This model has been effective for the Communications Sector. In the decades since wireless voice service emerged, we have progressed through generations of technology, supporting an explosion of data driven services from streaming video to Smart Cities. Just as it did when developing 2G, 3G, and 4G standards—dedicating enormous effort to improving security through encryption as well as multi-factor authentication and sophisticated validation techniques—industry groups are aggressively building security into fifth-generation ("5G") wireless. The industry continues to develop state-of-the-art tools to detect, isolate, and mitigate threats, and proactively defend networks and devices using firewalls, intrusion detection, monitoring, and anti-virus/anti-malware software. 5G and the IoT present a transformative opportunity, and industry is working tirelessly to make security a foundational element of next generation technology.

Challenges remain. Evolving cyber threats come from varied, global actors: nation-states, criminal syndicates, hacktivists and terrorists. Vulnerabilities are being leveraged crassly for monetary gain. Consumers and companies hear daily about attacks and risks. End users, including the government, still lag in basic cyber hygiene. And now, U.S. regulators are considering burdensome obligations that could stymie innovation and lead to fragmentation.

Notwithstanding these challenges, CTIA sees great opportunity. Innovation is occurring in network design, device security, authentication, and information sharing. The entire information and communications technology ("ICT") ecosystem is building on successes, including the National Institute of Standards and Technology's ("NIST's") *Cybersecurity Framework*.[4] Public-private partnerships are working, as the Department of Homeland Security ("DHS") and Information Sharing and Analysis Organizations ("ISAOs") begin the real work of collaboration. And consumers increasingly are using tools to secure devices and information.

Cybersecurity policy has come to an inflection point. The government must stay the course, building on a history of successful public-private partnerships. The United States must

---

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry. With members from wireless carriers and their suppliers to providers and manufacturers of wireless data services and products, the association brings together a dynamic group of companies that enable consumers to lead a 21st century connected life. CTIA members benefit from its vigorous advocacy at all levels of government for policies that foster the continued innovation, investment and economic impact of America's competitive and world-leading mobile ecosystem. The association also coordinates the industry's voluntary best practices and initiatives and convenes the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] Executive Order 13718 (Feb. 9, 2016) established the Commission on Enhancing National Cybersecurity.

[3] CTIA does not comment on insurance, research and development, or state and local government cybersecurity.

[4] Framework for Improving Critical Infrastructure Cybersecurity, at 1 (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf ("Cybersecurity Framework").

lead internationally by promoting international norms, supporting innovation and collaboration, and discouraging regulation. United States cyber policy must adhere to certain core values, identified in Part X below, as the Commission charts the future in a new administration. CTIA and its members look forward to continuing their partnerships with the government to maintain the security of our nation's communications infrastructure.

II. The United States Has Developed Effective Cybersecurity Policy Centered On Public-Private Partnerships.

CTIA shares the Commission's goal to "bolster[] partnerships between Federal, state, and local government and the private sector in the development, promotion, and use of cybersecurity technologies, policies, and best practices."[5] Such public-private partnerships have been the bedrock of federal cyber policy, and should continue. As Secretary of State John Kerry explained, the United States' effective "multi-stakeholder approach is embodied in a myriad of institutions that each day address Internet issues and help digital technology to be able to function."[6]

The past five years have seen federal activity in cybersecurity at all levels. The President has issued several Executive Orders. In addition to the Order establishing the Commission, key efforts include Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," and Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing." Each increased awareness and urgency about cybersecurity and recognized the importance of partnership and collaboration.

Before these efforts, the private sector successfully worked together and with government to advance the nation's cyber posture against constantly-changing threats. Recently, NIST led a partnership with the private sector to create the *Cybersecurity Framework*, yielding a voluntary, risk-based strategy that has been lauded and is being widely adapted. NIST eschewed a "one-size-fits-all" approach in favor of voluntary risk management because "[o]rganizations will continue to have unique risks—different threats, different vulnerabilities, different risk tolerances—and how they implement the practices in the framework will vary."[7] NIST's *Cybersecurity Framework* was successful because it resulted from a public-private collaboration. Executive Order 13636 instructed that NIST "incorporate voluntary consensus standards and industry best practices to the fullest extent possible" and "be consistent with voluntary international standards" when possible.[8]

The *Cybersecurity Framework* helps companies address risk in a cost-effective way and without regulation. The *Cybersecurity Framework* "jumpstarted a vital conversation between critical infrastructure sectors and their stakeholders. . . . [and] [t]hey can now work to understand the cybersecurity issues they have in common and how those issues can be addressed in a cost-

[5] Charter of the Commission on Enhancing National Cybersecurity, § 3, *available at* https://www.nist.gov/cybercommission/ ("Commission Charter").
[6] John F. Kerry, Secretary of State, Remarks at Korea University, Seoul, South Korea, *An Open and Secure Internet: We Must Have Both* (May 18, 2015), http://www.state.gov/secretary/remarks/2015/05/242553.htm.
[7] *Cybersecurity Framework*, at 2.
[8] Executive Order 13636, 78 Fed. Reg. 11739, *Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2013).

effective way without reinventing the wheel."[9] It provides a common taxonomy "enable[s] security leaders to effectively communicate practices, goals, and compliance requirements with third-party partners, service providers, and regulators."[10] It has become a baseline for sector plans and international efforts.

Beyond NIST, DHS is a critical convener. As the sector-specific agency for cybersecurity in the Communications Sector, it plays a key role helping secure national communications infrastructure. Its efforts include the Critical Infrastructure Cyber Community C^3 ("C^3"),[11] and the Communications Sector Coordination Council ("CSCC").[12] The Science and Technology Directorate ("S&T") is the DHS's research and development arm. S&T works with other Federal agencies, state, local, and tribal governments, universities, and private industry on research and development in cybersecurity to secure the nation's cyber and critical infrastructure. DHS does other security tasks as needed; for example at Congressional direction, DHS is looking at mobile security threats and defenses.[13]

Though DHS is the sector-specific agency for the Communications Sector, the Federal Communications Commission ("FCC") also is looking at cybersecurity. Groups like the Communications Security, Reliability, and Interoperability Council ("CSRIC") [14] and Technical Advisory Council ("TAC")[15] study cybersecurity. The *Cybersecurity Framework* has been voluntarily adapted throughout the Communications Sector through a massive effort reflected in CSRIC IV's *Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report*.[16] And as noted below, the FCC has started to pursue regulatory activities that threaten fragmentation and can erode collaboration.

Congress has played an important role, passing long-sought legislation to remove barriers. Recently, Congress passed the Cybersecurity Information Sharing Act of 2015 ("CISA"), which facilitates industry information sharing with the federal government and one

---

[9] NIST Press Release, *NIST Releases Cybersecurity Framework Version 1.0* (Feb. 12, 2014), http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.

[10] PricewaterhouseCoopers, WHY YOU SHOULD ADOPT THE NIST CYBERSECURITY FRAMEWORK 4 (2014), *available at* https://www.pwc.com/us/en/increasing-it-effectiveness/publications/asssets/adopt-the-nist.pdf.

[11] The C^3 Voluntary Program aims to "be the coordination point with the Federal Government for critical infrastructure owners and operators interested in improving their cyber risk management processes." DHS, *Critical Infrastructure Cyber Community C^3 Voluntary Program*, http://www.dhs.gov/about-critical-infrastructure-cyber-community-c%C2%B3-voluntary-program.

[12] U.S. Communications Sector Coordinating Council, http://www.commscc.org/.

[13] Department of Homeland Security, *Mobile Security Threats and Defenses*, Request for Information, Solicitation Number QTA00NS16SDI0003 (Aug. 5, 2016), https://www.fbo.gov/index?tab=documents&tabmode=form&subtabcore&tabid=f5ea833b29f037afdabdaa7260dc9620 (Responses were due Aug. 22, 2016).

[14] *See* Federal Communications Commission, *Communications Security, Reliability and Interoperability Council V*, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability#block-menu-block-4.

[15] *See* Federal Communications Commission, *Technological Advisory Council*, https://www.fcc.gov/general/technological-advisory-council.

[16] Available at http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_WG4_Report_Final_March_18_2015.pdf

another.[17] Congress also passed legislation to support research and development and address cybersecurity workforce.[18] The Commission should build federal policy on these successes.

III. The Communications Sector Has Been Fully Engaged On Critical Infrastructure Cybersecurity And Is Leading In 5G Innovation And Security.

The RFI asks about "effective private sector and government approaches to critical infrastructure protection in light of current and projected trends in cybersecurity threats and the connected nature of the United States economy."[19] The Communications Sector, as critical infrastructure, has made cybersecurity a top priority. It dedicates enormous effort to improve networks, devices, and defenses, as networks transitioned from 2G to 4G, and look ahead to 5G.

A. The Communications Sector Relies On Partnerships, Evolving Standards And Best Practices, And Information-Sharing To Meet Security Needs.

Because so much critical infrastructure is controlled by the private sector, collaboration with the public sector is vital. Industry regularly collaborates with the federal government. It helped develop the NIST *Cybersecurity Framework*, which according to one report, thirty percent of U.S. organizations now use. Use is projected to reach fifty percent by 2020.[20] Collaboration works. The Commission need not reinvent the wheel—it can build on existing policy, public-private partnerships, and voluntary standards.

1. The Wireless and Internet Ecosystems Use A Multilayered Approach To Security.

In the Communications Sector, each layer (internet service providers ("ISPs"), network operators, operating systems ("OS") developers, manufacturers, and application developers, among others) contributes to security. This multilayered approach is not only effective, it is vital to supporting efforts throughout the internet and wireless ecosystem. Communications infrastructure is a complex and interrelated "system of systems." In mobile, for example, there is an upstream segment relying on spectrum, towers, backhaul facilities; a transmit segment across the network; and a downstream segment relying on sophisticated mobile devices. Vulnerability in any one of these segments undermines efforts to protect the others.

All contributors to the internet and wireless ecosystems—large and small, domestically and worldwide—share responsibility for multilayered protection. Major OS providers work with application developers on application security, and many OS application stores do a good job of screening for bad applications. Network operators monitor traffic and combat threats. Over-the-top applications add layers of security. Industry is identifying and refining threat indicators, making technical improvements to network and communications infrastructure, and addressing remediation and notification. CTIA has released several White Papers addressing cybersecurity

---

[17] Cybersecurity Act of 2015, Pub. L. No. 114-113 (signed Dec. 18, 2015).
[18] *See* Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274 (signed Dec. 18, 2014); Cybersecurity Workforce Assessment Act, Pub. L. No. 113-246 (signed Dec. 18, 2014).
[19] *Commission Charter*, § 4(b).
[20] *See* News Release, NIST, *Cybersecurity "Rosetta Stone" Celebrates Two Years of Success* (Feb. 18, 2016), *available at* http://nist.gov/itl/acd/cybersecurity-rosetta-stone-celebrates-two-years-of-success.cfm.

issues,[21] developed through shared member experience and collaborative research. Industry participants, including those in the global ICT market, undertake research and release their own papers and analyses.[22] Industry's extensive research yields new tools to improve security, including device management, anti-theft, anti-malware, browsing protection, app reputation checking, call/short message service ("SMS") blocking and scanning, and firewalls.

This multilayered approach is supporting security in 5G. 5G Americas has told the FCC, "security has been a design component in third and fourth generations of mobile broadband technologies, and is increasingly required by its members' customers throughout the ecosystem. Security is now a market imperative."[23] As Ericsson states, "[c]ellular systems pioneered the creation of security solutions for public communication, providing a vast, trustworthy ecosystem – 5G will drive new requirements due to new business and trust models, new service delivery models, [and] an evolved threat landscape . . . ."[24] Companies, researchers and standards bodies are architecting 5G security throughout the ecosystem.[25] Among other things, industry is looking at network function virtualization, software defined networks, hardware configurations, the role of the cloud, and network management innovations. Each layer of the ecosystem will have a role to play in securing 5G.

2. The Communications Sector Relies on Flexible, Global Standards and Best Practices.

National and international standards groups develop collaborative standards and best practices that help secure systems. These groups bring together technical experts from around the world, and have supported mobile innovation, global interoperability, and scale for decades.

- The 3rd Generation Partnership Project ("3GPP"), an international organization uniting seven telecom standard organizations,[26] developed encryption standards to protect data in transit as it moves from the mobile device to the mobile network. 3GPP has worked with

[21] *See* Appendix attached hereto for selected publications, filings and cites, including: TODAY'S MOBILE CYBERSECURITY: INFORMATION SHARING (September 2014) ("CTIA White Paper on Information Sharing"); MOBILE CYBERSECURITY AND THE INTERNET OF THINGS: EMPOWERING M2M COMMUNICATION (May 2014) ("CTIA White Paper on IoT"); TODAY'S MOBILE CYBERSECURITY: INDUSTRY MEGATRENDS & CONSUMERS (May 2013), ("CTIA White Paper on Industry Megatrends"); TODAY'S MOBILE CYBERSECURITY: BLUEPRINT FOR THE FUTURE (February 2013); *TODAY'S MOBILE CYBERSECURITY: PROTECTED, SECURED AND UNIFIED* (October 2012) ("CTIA White Paper on Mobile Security").

[22] *See Verizon 2014 Data Breach Investigations Report* (2014), *available at* http://www.verizonenterprise.com/DBIR/; *Cisco Midyear 2014 Security Report* (2014), *available at* http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000502656; *Neustar Annual DDoS Attacks and Impact Report* (2014), *available at* http://2014-annual-ddos-attacks-and-impact-report.pdf.

[23] 5G Americas, Notice of Ex Parte, *Use of Spectrum Bands Above 24 GHz for Mobile Radio Services*, GN Docket No. 14-177, at 1-2 (filed Apr. 8, 2016), *available at https://ecfsapi.fcc.gov/file/60001568949.pdf*.

[24] Ericsson White Paper, *5G Security: Scenarios and Solutions*, Uen 284 23-3269 (June 2015), *available at* https://www.ericsson.com/res/docs/whitepapers/wp-5g-security.pdf.

[25] *See e.g.*, Günther Horn, Peter Schneider Nokia Networks, *Toward 5G Security*, *available at* http://resources.alcatel-lucent.com/asset/200292 (identifying technical questions and solutions, noting "5G activities in standardization bodies, in particular 3GPP, have already been scheduled").

[26] 3GPP's seven organizational partners are The Association of Radio Industries and Business, Japan; The Alliance for Telecommunications Industry Solutions, USA; China Communications Standards Association; The European Telecommunications Standards Institute; Telecommunications Standards Development Society, India; Telecommunications Technology Association, Korea; and Telecommunication Technology Committee, Japan.

Groupe Speciale Mobile Association ("GSMA") to develop a certification program for 3GPP's Security Assurance Methodology.

- The Internet Engineering Task Force ("IETF")—a community of network designers, operators, vendors, and researchers concerned with internet operations and evolution—sets international security-related standards.[27]
- The Alliance for Telecommunications Industry Solutions ("ATIS") fosters communication between carriers, customers, and manufacturers. The ATIS Network Performance, Reliability, and Quality of Service Committee recommends standards and technical reports related to security aspects of communications networks.[28]
- The Institute of Electrical and Electronics Engineers ("IEEE") has been a leader, launching a cybersecurity initiative to "(1) provide the go-to online presence for security and privacy (S&P) professionals; (2) improve the understanding of cybersecurity by students and educators; and (3) improve S&P designs and implementations by professionals."[29]

These and many other groups are working on 5G security. For example, IEEE is working on issues related to new wireless applications likely to run on 5G, such as security for dedicated short-range communications used by autonomous vehicles.[30] NIST is working on efforts related to 5G.[31] And the FCC's TAC is continuing to investigate cybersecurity issues related to IoT and 5G.[32] Alongside CTIA's Cybersecurity Working Group, these and other groups convene experts to develop and refine technical solutions that support innovation. Such voluntary consensus standards are critical, because they reflect the complexities of a global, innovative market, and promote flexibility, backward-compatibility, and interoperability.

3. The Communications Sector Actively Shares Vital Information.

Industry also shares best practices and keeps abreast of threats.[33] These extensive efforts are not always public-facing, but are critical. For example, mobile cybersecurity is supported by public-private forums like the National Cybersecurity and Communications Integration Center ("NCCIC"), the Communications Information Sharing and Analysis Center ("Comm-ISAC"), the Communications Sector Coordination Council ("CSCC"), and the National Security Telecommunications Advisory Committee ("NSTAC").[34]

---

[27] *See* IETF, https://www.ietf.org/about/.
[28] *See* ATIS, PRQC Mission, http://www.atis.org/0010/mission.asp.
[29] *See* IEEE, IEEE Cyber Security About Page, http://cybersecurity.ieee.org/about/.
[30] *See* John Kenney, Dedicated Short-Range Communications (DSRC) Standards in the United States, 99 Proceedings of the IEEE 7 (July 2011), *available at* http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5888501&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5888501.
[31] *See, e.g.*, NIST Communications Technology Laboratory, http://www.nist.gov/ctl/wireless-networks/5gnetworks.cfm. Other NIST efforts have looked at various aspects of mobile security.
[32] *See* TAC, Mar. 9, 2016 Meeting Presentation, 5-7 *available at* https://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting3916/TAC-Presentations-3-9-16.pdf.
[33] McAfee, MCAFEE LABS THREATS REPORT 2 (March 2016), *available at* http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2016.pdf ("Intel Security interviewed almost 500 security professionals to . . . . awareness is very high and that 97% of those who share cyber threat intelligence see value in it.").
[34] *See CTIA White Paper on Information Sharing*, at 13 (forums "make possible certain exchanges of information related to cybersecurity threats that can impact mobile communications.").

Information Sharing Analysis Centers ("ISACs") and Information Sharing and Analysis Organizations ("ISAOs") are influential in threat prevention, protection, response and recovery. Their success is the result of industry leadership and government support. The Administration, through Executive Order 13691, directs the DHS to encourage the development of ISAOs, recognizing that "[o]rganizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States."[35] A key goal of the DHS selected ISAO Standards Organization is to develop standards and best practices that are voluntary, transparent, actionable, and flexible. Likewise, CISA facilitates sharing between the public and private sectors about threats—bridging a barrier to cybersecurity. Advances in information sharing contribute to the relatively low rates of malware encounters as compared with much of the rest of the world.[36]

Sharing is even more vital now, as researchers scour devices and networks for vulnerabilities and parties with varied motives exploit them, including for financial gain. Recent news reports confirm that a longstanding "unofficial truce between cybersecurity researchers and companies" to permit remediation before public disclosure, has come under attack. [37] In a novel arrangement, an investment firm agreed to make claimed medical device vulnerabilities "public in exchange for giving the cybersecurity [research] firm a cut of the profits . . . from betting against the medical device maker's stock."[38] This is troubling because premature public disclosure can enable bad actors to do harm before a company can remediate the vulnerability. A multistakeholder process is underway at NTIA,[39] but as the ecosystem considers responsible disclosure policies, the government must help protect sensitive information and promote responsible information sharing and collaboration.

B. The Government Should Support Vital Partnerships and Industry Efforts.

The most effective government approach to critical infrastructure protection is to robustly promote private, collaborative efforts and voluntary standards. This model has worked well so far, and is the best way to meet emerging challenges in this rapidly changing environment. This preference for partnerships flows from longstanding federal policy of avoiding regulation of the internet and digital technology, using the lightest touch possible and deferring to innovators. As we look ahead, "policymakers should use a light touch to regulate legitimate use of digital

---

[35] Executive Order 13691, 80 Fed. Reg., 9,349, *Promoting Private Sector Cybersecurity Information Sharing*, §1 (Feb. 13, 2015).

[36] *See* Verizon, *2015 Data Breach Investigations Report*, at 19-20 (2015), *available at* http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf ("An average of 0.03% of smartphones per week—out of tens of millions of mobile devices on the Verizon network—were infected with 'higher-grade' malicious code. This is an even tinier fraction than the overall 0.68% infection rate reported.").

[37] A. Peterson, *A new hacker money-making strategy: Betting against insecure companies on Wall Street*, Washington Post (Sept 1, 2016) *available at* https://www.washingtonpost.com/news/the-switch/wp/2016/09/01/a-new-hacker-money-making-strategy-betting-against-insecure-companies-on-wall-street/.

[38] *Id.*

[39] NIST, *Multistakeholder Process: Cybersecurity Vulnerabilities* (Apr. 8, 2016), https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.

technology, and take a hard line on regulating illegitimate digital activity, such as cybercrime and online piracy."[40]

Not are public-private partnerships effective, such an approach is consistent with federal law, which requires the government to use voluntary standards wherever possible. Pursuant to 19 U.S.C. § 2532, "[n]o Federal agency may engage in any standards-related activity that creates unnecessary obstacles to the foreign commerce of the United States."[41] Similarly, Office of Management and Budget ("OMB") Circular A-119 requires agencies to use voluntary standards in lieu of developing their own—"maintain[ing] a strong preference for using voluntary consensus standards over government-unique standards in Federal regulation and procurement."[42] These policies are codified in the National Technology Transfer and Advancement Act of 1995 ("NTTAA"), which states that "all Federal agencies and departments shall use technical standards that are developed or adopted by voluntary consensus standards bodies, using such technical standards as a means to carry out policy objectives or activities determined by the agencies and departments."[43] Where the government has pursued this approach, it has been widely successful. The government should support the Communications Sector's existing, aggressive activity, and eschew regulation or mandates.

IV. The Internet of Things, Powered by 5G Wireless, Will Drive The Digital Economy, And Industry Is Working Tirelessly To Ensure Its Security.[44]

The RFI seeks input on the Internet of Things, to "ensure[] that cybersecurity is a core element of the technologies associated with the Internet of Things and cloud computing, and that the policy and legal foundation for cybersecurity in the context of the Internet of Things is stable and adaptable."[45] Cybersecurity is being built into the 5G network and all aspects of IoT. The government should promote innovation and resist regulatory impulses that limit innovation.

A. As IoT Evolves, Industry Is Addressing Security.

The 5G network will bring unprecedented data rates and mobile access, accommodating billions of connected devices. "The IoT will provide greater efficiency by automating tasks, exchanging information, performing updates, making adjustments, maintaining thresholds and comparing variances. Machines will communicate directly with one another based on intelligent algorithms that help liberate us from routine tasks, improve end-user quality of life, reduce

---

[40] Information Technology & Innovation Foundation, *Clinton vs. Trump: Comparing the Candidates' Positions on Technology and Innovation*, at 18 (Sept. 2016), *available at* http://www2.itif.org/2016-clinton-vs-trump.pdf?_ga=1.265389769.71842715.1473264672.

[41] 19 U.S.C. § 2532.

[42] OMB Circular A-119: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities, at 4 (January 27, 2016).

[43] NTTA, Pub. L. No. 104-113, § 12(d), 110 Stat 775 (1995).

[44] The RFI seeks input on "[e]merging technology trends and innovations; the effect these technology trends and innovations will have on the digital economy; and the effect these technology trends and innovations will have on cybersecurity." NIST RFI, 81 Fed. Reg., at 52828.

[45] *Commission Charter*, § 4(a).

complexity and cycle time, improve efficiency and often enhance safety."[46] Experts estimate that there will be 50 billion connected devices by 2020.[47]

Opportunities from IoT are limitless. The FTC identified several benefits in areas including health; smart homes; and autonomous cars, and also noted concerns about IoT, including security.[48] As with any new technology, there are benefits and risks. But as communications technology evolves, so does security. Industry groups are aggressively building security into 5G, just as it did when developing 2G, 3G, and 4G standards. The private sector continues to explore effective ways to minimize risks in IoT, and it can do so faster and better than any agency. The Communications Sector designs products and systems with security in mind, incorporating the latest security technology and features into underlying infrastructure. Intel Corporation for example—which develops the chips for millions of IoT devices—is hard at work to deliver a roadmap of integrated hardware and software products to meet IoT security demands.[49] Because IoT will rely on wireless connectivity, the mobile industry is investing in security solutions—driving innovation through advances in monitoring and vulnerability scans, advanced security technology standards, enhancements to security policies and risk management, and advances in monitoring of specific cyber threats.[50]

B. The Government Should Resist Regulatory Impulses That Will Stymie IoT Innovation.

Existing policy frameworks should inform but not mandate policy in the IoT context. Generally, new IoT-specific regulation is unnecessary and could hamper the development of IoT technologies. Rather, government "will need to bring smart policies to the table to promote the adoption of important productivity-enhancing technologies" and "partner with the private sector in enabling the robust development and such of such technologies."[51]

The White House Office of Science and Technology Policy has said the White House looks at IoT "from a lens of playing a supportive role."[52] And Senate Commerce Committee Chairman John Thune (R-SD) has advocated for "the same light touch" treatment that "caused the Internet to be such a great American success story," and against reactionary, "government

---

[46] *CTIA White Paper on IoT*, at 5.
[47] FTC Staff Report, *Internet of Things—Privacy & Security in a Connected World* (January 2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
[48] *Id.* at ii.
[49] *See, e.g.*, Intel Corporation, *IoT and Scalability on Intel IoT Platform*, http://www.intel.com/content/www/us/en/internet-of-things/iot-platform.html (recognizing that "[s]ecurity is fundamental" so Intel is "optimizing [its] product roadmap to work seamlessly together with building blocks from the ecosystem to address the key challenges solutions providers are facing when implementing IoT including . . . security.").
[50] *See CTIA White Paper on IoT*, at 15 ("The industry manages M2M cybersecurity through 24/7 monitoring and threat assessment; design and testing; encryption; vulnerability management; and policy/data sharing.").
[51] Information Technology & Innovation Foundation, *Clinton vs. Trump: Comparing the Candidates' Positions on Technology and Innovation*, at 18 (Sept. 2016), *available at* http://www2.itif.org/2016-clinton-vs-trump.pdf?_ga=1.265389769.71842715.1473264672.
[52] Daniel Correa, Senior Advisor, Office of Science and Technology Policy, White House, quoted in D. Samuelson, *What Washington Really Knows About the Internet of Things*, Politico (June 29, 2015), http://www.politico.com/agenda/story/2015/06/internet-of-thingscaucus-legislation-regulation-000086#ixzz49DqAY1BW.

knows best" IoT regulation.[53] Thus, the government should resist the temptation to adopt regulations, and instead adhere to its flexible approach centralized around voluntary compliance and industry best practices. This approach allows the industry to respond instantly to changes in the dynamic IoT ecosystem, where devices will communicate with one another.

As it pioneers 5G, the industry is building security into the core infrastructure for IoT, and manufacturers and innovators are encouraged to build security into devices and their connections. The government should avoid demanding singular solutions that could fragment the market or limit flexibility. The industry's main concern is that oversight and controls remain flexible and supportive of this nascent market so that it can realize its promise to make peoples' lives safer and easier, and benefit society.[54]

V. Public Awareness and Good Cyber Hygiene Are Critical, And Will Benefit From Industry Leadership Rather Than Mandates.

The Commission is looking at ways to improve "broad-based education of commonsense cybersecurity practices for the general public."[55] Education is the cornerstone of effective security because technical and hardware solutions change and can be undermined by human error. Simple, common sense precautions will go a long way toward improving security. And, new security tools abound, with innovations like the smartphone "kill switch,"[56] device blacklisting, and new methods of authentication. There also are tools for consumers to address risks from apps that seek access to data or alter the function or security of their devices.[57] Consumers should be encouraged to use them.

Education is vital, because "with consumers in control, the stakes are higher than ever for education that encourages consumers and end users to adopt security-minded behaviors."[58] In mobile, that includes learning about "the importance of, and the methods for, installing and using a suite of protective measures (*e.g.*, strong passwords, anti-virus software, firewalls, intrusion detection systems ("IDS"), encryption) and update as available."[59] Often, incidents are preventable, and risks could have been mitigated by prudent consumer behavior such as avoiding password reuse, using widely-available password management programs, passphrases (a phrase

---

[53] Senate Commerce Committee Chairman John Thune Majority Statement, *The Connected World: Examining the Internet of Things: Hearing Before the S. Comm. On Com., Sci., & Transp*., 114th Cong. (Feb. 11, 2015), *available at* http://www.commerce.senate.gov/public/index.cfm/hearings?Id=D3E33BDE-30FD-4899-B30D-906B47E117CA&Statement_id=F58152BF-3E3B-4B28-A10B-5C4A13793473.

[54] *CTIA White Paper on IoT*, at 19.

[55] *Commission Charter*, § 4(a).

[56] *See* CTIA, *Smartphone Anti-Theft Voluntary Commitment* (July 2016), *available at* *http://www.ctia.org/docs/default-source/default-document-library/stolen-phone-commitment-new.pdf* ("The following network operators, device manufacturers and operating system companies fulfilled part 1 section B of the Commitment: Apple Inc.; Assurant; Asurion; AT&T; Google Inc.; HTC America Inc.; Huawei Device USA, Inc.; LGE Mobile Research U.S.A., LLC; Microsoft Corporation; Motorola Mobility LLC; Samsung Electronics America, Inc.; Sprint Corporation; T-Mobile USA; U.S. Cellular; Verizon and ZTE USA Inc.").

[57] CTIA, *Consumer Security & Privacy Tips* (November 2015), http://www.ctia.org/yourwireless-life/consumer-tips/tips/consumer-security-privacy-tips.

[58] *CTIA White Paper on Industry Megatrends*, at 2.

[59] FCC CSRIC, Working Group 2A: Cyber Security Best Practices, at 91 (2011), *available at* http://www.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf.

condensed by removing the spaces between words) instead of traditional passwords, and enabling two-factor authentication.[60]

As the government and private sector work to improve cyber hygiene, it must keep in mind that not all consumers have the same needs, desires or capabilities. Many favor ease over security. For example, when asked in a recent survey by Carnegie Mellon University's Security and Privacy Institute, CyLab[61] what they found most frustrating about password management, 20 percent cited remembering different passwords for various accounts, 18 percent satisfying complex password requirements, 15 percent the requirement to regularly change a password, and 12 percent getting locked out following several incorrect attempts.[62]

Consumer expectations about security are changing, and CTIA has observed the effectiveness of consumer education firsthand. Recently, CTIA found that sixty-nine percent of wireless consumers use PINs/passwords on their smartphones, up thirteen percent from 2015, and up thirty eight percent from the first survey in 2012. Likewise, fifty-one percent have built-in remote lock and erase software installed on their smartphones, up forty-two percent from 2015, and up thirty-one percent from 2012.[63] Evolving threats mean that responses must evolve as well. This makes it important for regulators to resist mandating solutions that override or ignore complex end user preferences and behavior or deprive industry of flexibility necessary to meet these ever-changing threats.

Government mandates will do more harm than good. Technical solutions change too quickly to support mandates, and required communications about risk, incidents, or solutions can result in over-notification that numbs people to real risks. Studies confirm that customers experiencing notice fatigue fail to appreciate the most important notices affecting customer privacy.[64] Data from Europe further suggest that providing customers frequent notices results in customer annoyance and may deter customer behavior online.[65] The government should support and amplify private efforts to raise awareness of available solutions.

---

[60] *See* R. Condon, *Alternatives to Passwords: Replacing the Ubiquitous Authenticator*, TechTarget (Dec. 29, 2011), http://searchsecurity.techtarget.com/magazineContent/Alternatives-to-passwords-Replacing-the-ubiquitous-authenticator (highlighting security benefits of password management software and two-factor authentication); Jeff John Roberts, *Here's a Better Way to Create a Strong Password You Will Remember*, Fortune (Aug. 15, 2016), *available at* http://fortune.com/2016/08/15/passwords/ (suggesting passphrases).

[61] Daniel Tkacik, *Users' Perceptions of Password Security Do Not Always Match Reality*, CyLab News (May 11, 2016), *available at* https://www.cylab.cmu.edu/news_events/news/2016/users-perceptions-of-password-security-do-not-always-match-reality.html.

[62] Ian Barker, *Frustration with Conventional Password Management Leads to Risky Behavior*, BetaNews (April 2016), http://betanews.com/2016/04/20/password-frustration/.

[63] Dr. Robert Roche, *Survey Shows Americans Follow Wireless Companies' Consumer Education Efforts on Mobile Security*, (July 21, 2016), *available at* http://www.ctialatest.org/2016/07/21/survey-mobile-security/.

[64] *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S J. L. & Pol'y for the Info. Soc'y 543 (2008) (calculating the costs of time spent reading privacy notices and suggesting that the frequency and length of policies are problematic); FTC, *Mobile Privacy Disclosures: Building Trust Through Transparency* 18 (Feb. 2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-throughtransparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf (noting the importance of ensuring that information does not become "too complex to be useful").

[65] *See* Ronald E. Leenes & Eleni Kosta, *Taming the Cookie Monster with Dutch Law—A Tale of Regulatory Failure*, 31 COMP. L. & SEC. REV. 317, 317 (2015) (describing a Dutch regulation causing "widespread deployment of

VI. Increasingly Global Challenges Demand U.S. Leadership On Cybersecurity Standards, Criminal Prosecutions, And Norms For State Action.

As the ICT and IoT become ever more global, it becomes harder to maintain an innovative, interoperable and secure ecosystem. Challenges to communications networks are varied: potential fragmentation from divergent international efforts, as well as security threats from global nation-states, terrorists and criminals. The United States can and should lead on both fronts.

In terms of interoperability and connectivity, networks are challenged by their global nature. Operators have traditionally relied on a closed, trust-based system supporting international communications. As key connection points become increasingly global, challenges arise when points are under foreign control and could be manipulated by those seeking to do harm. Shaken trust among internet and wireless network operators undermines collaboration and can harm security.

Likewise, some countries seek to use the ITU and other settings to promote favorable standards. Although cybersecurity should be pursued globally, it must also remain consistent with U.S. values, which promote flexibility and market-driven innovation. The Obama Administration has acknowledged recent efforts by G-20 leaders "to address security risks, threats, and vulnerabilities in the digital economy, including through application of risk-based cybersecurity approaches."[66] This commitment "echoes U.S. efforts to promote risk-based cybersecurity approaches through the President's Executive Order on Promoting Critical Infrastructure Cybersecurity and the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity"[67] and should be encouraged.

The United States must ensure that international organizations like the G-20 follow through with their commitments, including to "preserv[e] the global nature of the internet as an engine for growth" and the "commitment to the free flow of information, ideas, and knowledge across borders."[68] Forced data localization and other domestic rules, some in the name of security, make it hard to operate. As Secretary of State John Kerry explained, such requirements "create huge obstacles to multinational business at a time when speed is of the essence and cross-border enterprises are major engines of growth."[69] Claims that data localization rules bolster cybersecurity interests are false, and the government should flatly reject such proposals. Data localization requirements hinder digital trade without providing greater security. "Balkanized markets and networks lead to: slower economic growth, less consumer choice and higher prices,

---

annoying banners, popup screens, and 'cookie walls'" amounting to "regulatory failure"); J. Hayes, *Cookie Law—Will It Rumble or Crumble?*, Engineering & Technology (Aug. 21, 2012), http://eandt.theiet.org/magazine/2012/08/cookie-law.cfm (cookie law "may actively deter [people] from 'entering' online stores, or make them suspicious of otherwise legitimate sites").

[66] White House Fact Sheet, *The 2016 G-20 Summit in Hangzhou, China* (Sept. 5, 2016), *available at* https://www.whitehouse.gov/the-press-office/2016/09/05/fact-sheet-2016-g-20-summit-hangzhou-china.

[67] *Id.*

[68] *Id.*

[69] John F. Kerry, Secretary of State, Remarks at Korea University, Seoul, South Korea, *An Open and Secure Internet: We Must Have Both* (May 18,2015) http://www.state.gov/secretary/remarks/2015/05/242553.htm

higher global operating costs, and less security."[70] Voluntary international standards—including various ITU recommendations and standards developed by groups like IETF and 3GPP—will prevent balkanization and advance U.S. cybersecurity objectives.

These international challenges make it vital that the United States lead, and set an example that promotes private innovation over state control. Ambassador Terry Kramer, U.S. Head of Delegation to the World Conference on Internet Communications correctly recognized, "our international telecommunications and internet sectors are flourishing . . . precisely because it is an open platform—with open standards-setting, open markets, open networks and the free flow of ideas, content and commerce that is carried over those networks."[71] The U.S. must act now to preserve the open platform internationally. To address deglobalization of the ICT sector, the U.S. Chamber of Commerce urges governments to embrace a globalized ICT sector, promote market competition, promote transparency, and allow commercial procurers to set requirements.[72]

The United States must promote international harmonization and help build trust in network connections. It must continue to work internationally and through standards bodies, and avoid domestic regulation so that standards do not become fragmented. Some technical solutions are only effective when deployed ubiquitously. For example, Secure Border Gateway Protocol extension ("BGPSEC") is intended to ensure that the assignment path for en-route data is legitimate and not misrouted by mistake or maliciously. BGPSEC depends on several actions completed by members of the ICT community, including internet registries. Ubiquitous deployment can only be achieved through consensus, not regulation.

Ubiquity and interoperability are far from the only challenges. The United States must lead cooperative global prosecutions of cyber criminals, and promote international norms that build security and trust. Despite increased reports of cybercrime, it is hard to secure convictions. An article in the International Journal of Cyber Criminology credits this phenomenon to "trans-jurisdictional barriers, subterfuge, and the inability of key stakeholders in criminal justice systems to grasp fundamental aspects of technology aided crime."[73] As for nation-states, President Obama has acknowledged the challenge from cyber espionage and recently called for the global community to "start instituting some norms so that everybody's acting responsibly."[74] He observed that "[w]e're going to have enough problems in the cyber space with nonstate actors who are engaging in theft and using the internet for all kinds of illicit practices."[75]

---

[70] U.S. Chamber of Commerce, *Preventing Deglobalization: An Economic and Security Argument for Free Trade and Investment in ICT*, at 2 (Sept. 2016), *available at* https://www.uschamber.com/sites/default/files/documents/files/preventing_deglobalization_summary.pdf.

[71] Terry Kramer, Remarks to SAMENA (Sept. 9, 2012), *available at* http://www.state.gov/e/eb/rls/rm/2012/97545.htm.

[72] *See* Chamber of Commerce, *supra* note 69 (calling for like-minded governments to commit by formal agreement to abide by these principles).

[73] C. Brown, *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*, 9 INT'L J. OF CYBER CRIM. 1 at 56 (June 2015), *available at* http://www.cybercrimejournal.com/Brown2015vol9issue1.pdf.

[74] Politico, *Obama warns of cyber 'arms race' with Russia* (Sept. 5, 2016) http://www.politico.com/story/2016/09/obama-russia-cyber-arms-race-227732#ixzz4JU4jHZnF.

[75] *Id.*

The United States must address all of these issues aggressively through leadership and harmonization with the international community.

VII. Innovation In Identity and Access Management Will Drive Security Through Promising Approaches Like Biometrics.

The Commission will develop recommendations regarding "how best to bolster the protection of systems and data, including how to advance identity management, authentication, and cybersecurity of online identities, in light of technological developments and other trends."[76]

Identity and access management ("IAM") is a security discipline that ensures that the correct people and devices can access appropriate enterprise resources at the right times, for legitimate reasons. IAM will be critically important in the growing digital economy, as consumers use devices for more functions and organizations leverage mobility. It has been discussed for decades, by SANS Institute, NIST, and others. IAM was once a compliance, requirement-driven approach. Now "IAM is evolving into a risk-based program with capabilities focused on entitlement management and enforcement of logical access controls."[77] Traditional methods of access and identity control are not perfect. Current passwords, PINs and other requirements engender frustration among consumers, leading industry to seek alternatives. As discussed, a recent SecureAuth study found that Americans are "exasperated with conventional online password management," and revealed that "74 percent [of Americans] rely on means other than memory to manage their online passwords," including 35 percent that write down their passwords and another 25 percent that use the same password across several accounts.[78] Experts are therefore looking at two-factor authentication, including SMS and other mechanisms, to provide security despite lax consumer practices.[79]

"The IoT introduces the need to manage exponentially more identities than existing IAM systems are required to support. The security industry is seeing a paradigm shift whereby IAM is no longer solely concerned with managing people but also managing the hundreds of thousands of 'things' that may be required to connect to a network."[80] According to a European Commission report on IoT identities, "the issues of providing non-colliding unique addresses in a global scheme requires an infrastructure in place that supports highly dynamic devices that appear and disappear from the network at any time, move between different local and/or private networks and have the flexibility to either identify their uniquely or hide his/her identity, thus

---

[76] *Commission Charter*, § 4(a).

[77] Ernst & Young, *Identify and Access Management Beyond Compliance*, at 1 (May 2013), *available at* http://www.ey.com/Publication/vwLUAssets/Identity_and_access_management_-_Beyond_compliance/$FILE/Identity_and_access_management_Beyond_compliance_AU1638.pdf..

[78] Ian Barker, *Frustration with Conventional Password Management Leads to Risky Behavior*, BetaNews (April 2016), http://betanews.com/2016/04/20/password-frustration/.

[79] *See* Ron Condon, *Alternatives to Passwords: Replacing the Ubiquitous Authenticator*, TechTarget (Dec. 29, 2011), http://searchsecurity.techtarget.com/magazineContent/Alternatives-to-passwords-Replacing-the-ubiquitous-authenticator (highlighting security benefits of password management software and two-factor authentication); Jeff John Roberts, *Here's a Better Way to Create a Strong Password You Will Remember*, Fortune (Aug. 15, 2016), *available at* http://fortune.com/2016/08/15/passwords/.

[80] Cloud Security Alliance, *Identity and Access Management for the Internet of Things—Summary Guidance, IoT Working Group*, at 3 (Sept. 30, 2015), *available at* https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/identity-and-access-management-for-the-iot.pdf.

preserving privacy as needed. Whether managing smart sensors, connected parking meters, automobiles, or connected health devices, each must be addressable within the larger system and the name of the thing should be bound to a credential."[81]

IoT is in the early stages, but the Communications Sector is examining how IAM relates to other security required for an IoT-connected enterprise (*e.g.*, asset and cryptographic key management). Offerings abound from many major participants in the mobile ecosystem: Oracle, Blackberry, MobileIron, AT&T, and others. According to Forbes, "AT&T Halo is an identity and access management (IAM) platform which the company developed as an easier and more secure way for people to login to all of their mobile devices and computing systems."[82]

Biometric authentication is promising. The use of fingerprints, retinal scans, voice, hold promise for many mobile uses. Research is moving forward,[83] and experts are looking at how to use biometrics in different ways.[84] Samsung, for example, is "using fingerprint or iris scans for optimum security in their new devices."[85] Mobile banking is similarly deploying biometrics. Fingerprint biometrics (*i.e.*, fingerprint detection and swiping access) eliminate passwords and PIN codes, which users have grudgingly accepted over the past two decades.[86] Companies are also collaborating to build solutions and services.[87]

No solution will be perfect, but industry needs flexibility to explore options and experiment. Work is underway to set standards and best practices. The IETF is examining Authentication and Authorization for Constrained Environments ("ACE"),[88] including modifications to IoT protocols for authentication and authorization-related tasks. NIST has been a good catalyst, with several projects and research to support innovative approaches to IAM.[89] The government should avoid picking particular technology approaches and allow standard

---

[81] European Commission, *Internet of Things Factsheet Identification*, at 1 (2013), *available at* https://ec.europa.eu/digital-single-market/news/conclusions-internet-things-public-consultation.

[82] Steve Morgan, *AT&T Promises No More Passwords, PIN Codes, and Security Questions*, FORBES (May 5, 2016), *available at* http://www.forbes.com/sites/stevemorgan/2016/05/05/att-no-more-passwords-pin-codes-and-security-questions/#188977783b0d.

[83] *See e.g.*, S. Trewin, *Biometric Authentication on a Mobile Device: A Study of User Effort, Error and Task Disruption* (IBM Research Labs, 2012) (examining biometric authentication modalities—voice, face and gesture – as well as password entry, on a mobile device, to explore demands on user time, effort, error and task disruption.).

[84] *Study Says Mobile Payments Need Biometrics*, Security Magazine (June 19, 2016) (identifying palm vein, fingerprint, iris scan), http://www.securitymagazine.com/articles/87199-study-says-mobile-payments-need-biometrics; NerdWallet, *More Banks Turn to Biometrics to Keep an Eye on Security*, Nasdaq (May 23, 2016), http://www.nasdaq.com/article/more-banks-turn-to-biometrics-to-keep-an-eye-on-security-cm624871#ixzz4IOknMTRR.

[85] *See Iris Scanning Brings Added Security to Mobile*, Samsung Newsroom (Aug. 18, 2016), https://news.samsung.com/global/editorial-iris-scanning-brings-added-security-to-mobile.

[86] Steve Morgan, *AT&T Promises No More Passwords, PIN Codes, and Security Questions*, Forbes (May 5, 2016), *available at* http://www.forbes.com/sites/stevemorgan/2016/05/05/att-no-more-passwords-pin-codes-and-security-questions/#188977783b0d (describing AT&T's MobileKey technology).

[87] IBM, *AT&T and IBM Team Up for Mobile Cloud Security* (Oct. 5, 2015), https://www-03.ibm.com/press/us/en/pressrelease/47777.wss ("AT&T and IBM can deliver a scalable mobile solution to help protect corporate data and apps.").

[88] IETF, *Authentication and Authorization for Constrained Environments*, https://datatracker.ietf.org/wg/ace/documents/.

[89] NIST, *Identity Management and Access Control*, http://csrc.nist.gov/projects/iden_ac.html.

setting organizations and similar collaborative groups to take the lead. IAM will not lend itself to regulatory commands or universal approaches, as conventional wisdom can quickly change.

VIII. The Nation Faces A Scarcity of Skilled Cyber Workers, And The Communications Sector is Addressing The Challenge.

Scarcity in the cyber workforce affects the government and the private sector. The Obama Administration has long been concerned that "there are not enough cybersecurity experts within the Federal Government or private sector."[90] Seventy-one percent of respondents in a recent study reported that the shortage in cybersecurity skills does "direct and measureable damage" and ninety-seven reported their organization's board of directors now view cybersecurity as important."[91] OMB's 30-day "Cybersecurity Sprint" revealed: (1) "Federal agencies' lack of cybersecurity and IT talent is a major resource constraint that impacts their ability to protect information and assets;" and (2) "[a] number of existing Federal initiatives address this challenge, but implementation and awareness of these programs are inconsistent."[92] The next administration must work with Congress and the private sector 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."[93]

Industry is not waiting on government. For example, the FCC's CSRIC V Working group 7 ("WG7") is developing recommendations for the FCC to improve the security of the nation's critical communications infrastructure by enhancing transparency, skill validation, and best practices in recruitment, training, retention, and job mobility of personnel in cybersecurity.[94] This working group will leverage existing work to enhance the workforce, including:

- Demonstrating the application of the National Cybersecurity Workforce Framework ("NCWF") to the common and specialized work roles with in the communications sector;
- Identifying any gaps or improvements in the NCWF for evolving work roles or skill sets that should be included in sector members' workforce planning; and
- Identifying, developing, and recommending 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.

---

[90] White House, *The Comprehensive National Cybersecurity Initiative*, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

[91] McAfee-Intel Security Report, *Hacking the Skills Shortage—A Study of the International Shortage in Cybersecurity Skills*, at 4, 6 (May 2, 2016), *available at* http://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf.

[92] Shaun Donovan, Beth Cobert, Michael Daniel, and Tony Scott, *Strengthening the Federal Cybersecurity Workforce*, White House Blog (July 12, 2016), *available at* https://www.whitehouse.gov/blog/2016/07/12/strengthening-federal-cybersecurity-workforce ("White House Workforce Blog").

[93] *Id.*

[94] CSRIC, *Interim Report—Analysis of Applicability of the National Cybersecurity Workforce Framework (NCWF) to the Communications Sector and Identification of Gaps*, at 12 (March 2016), *available at* https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability#block-menu-block-4.

WG7's Interim Final Report concluded, "we are still in the early days of addressing the development of a skilled cybersecurity workforce that can meet our needs," and that WG7 "plans to further collaborate across academia, industry and Government to develop recommendations and identify best practices that can be leveraged to enhance cybersecurity workforce planning."[95]

CTIA applauds federal efforts, including the Administration's Federal Cybersecurity Workforce Strategy, which seek to identify cybersecurity workforce needs, expand the workforce through education and training; recruit, retain and develop talent for federal service.[96] The Administration identifies "engaging Federal and non-Federal stakeholders [to] provide the resources necessary to establish, strengthen, and grow a pipeline of cybersecurity talent" represents a meaningful first step.[97] CTIA looks forward to collaborative efforts to implement the Federal Cybersecurity Workforce Strategy.

IX. As the Government Remains Under Attack, Federal Governance Must Improve to Protect Government Functions, Data and Trust.[98]

The U.S. government is under constant threat of attack from hackers seeking sensitive financial or identity information, intellectual property and intelligence. Last year, hackers gained access to IRS data of more than 700,000 taxpayers.[99] The 2015 hack of OPM exposed personal information of 22 million current and former federal employees.[100] These attacks undermine confidence in the government's ability to protect information. Thirty-nine percent of people polled in a 2015 survey from Unisys Security Insights, which measures global data security concerns, indicated that they think it's "likely" that personal information of theirs stored by government agencies will be accessed without their consent before the year is through.[101] As a user of ICT and a target, the government can do a better job including security into digital strategy, educating its user community, and managing mobile.

To do so, the government must be a true partner with the private sector, on which it relies for devices, connectivity, and managed services.[102] The government can strengthen governance.

---

[95] *Id.* at 19.

[96] Memorandum for Heads of Executive Departments and Agencies, *Federal Cybersecurity Workforce Strategy*, Executive Office of the President, OMB at 3 (July 12, 2016), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-15.pdf.

[97] *White House Workforce Blog*.

[98] Executive Order 13718, 81 Fed. Reg. 7,441, § 3(b)(i)(C) (The Commission is to develop recommendations for "a governance model for managing cybersecurity risk, enhancing resilience, and ensuring appropriate incident response and recovery in the operations of, and delivery of goods and services by, the Federal Government.").

[99] Kevin McCoy, *Cyber Hack Got Access to Over 700,000 IRS Accounts*, USA Today (Feb. 26, 2016), *available at* http://www.usatoday.com/story/money/2016/02/26/cyber-hack-gained-access-more-than-700000-irs-accounts/80992822/.

[100] Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, The Washington Post (July 9, 2015), *available at* https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

[101] Unisys Security Insights, *Unisys Security Insights—How US Consumers Feel About Personal Data Security, Ranked by Industry and Biometrics as a Security Measure*, at 5 (2015), *available at* http://assets.unisys.com/|Documents/Microsites/UnisysSecurityInsights/USI_150227_USreport.pdf.

[102] Executive Order 13718, 81 Fed. Reg. 7,441 §3(b)(i)(D) (The Commission is to develop "strategies to overcome barriers that make it difficult for the Federal Government to adopt and keep pace with industry best practices.").

- *First*, education is critical, and the government should invest in educating its personnel. GAO agrees: "it is important that an appropriate level of awareness [be] achieved among consumers who use mobile devices on a regular basis."[103] As a user and beneficiary of ICT and mobility, the government plays a key role in the multilayered ecosystem and must do its part to ensure its own security.
- *Second*, the government should be cautious about using procurement to drive change in the private sector. Standards must remain voluntary and flexible—not cemented in regulatory obligations or procurement standards that tie industry's hands.
- *Finally*, the government should encourage voluntary, third party standards and innovation. Such approach is consistent with the NTTA and OMB Circular A-119, which require federal agencies to "use voluntary consensus standards in lieu of government-unique standards in their procurement and regulatory activities."[104]

Much work remains to leverage the accomplishments of NIST's *Cybersecurity Framework*, activities at DHS, and in ISAOs. The government and private sector are still grappling with full implementation of CISA, including automated threat indicators. The government should strive to coordinate and consolidate the many existing efforts, allowing the private sector to invest in technology and tools to help the private sector and government improve their cybersecurity preparedness and responsiveness.

X. Conclusion: At This Inflection Point, Core Principles Have Emerged To Guide Federal Policy.

CTIA and its members have partnered with DHS, NIST, NTIA, FCC, and others to meet evolving cyber threats to the critical infrastructure. After significant progress, federal cybersecurity policy has arrived at an inflection point. The international community is moving ahead, and federal agencies are exploring regulation and other activities. This all comes as the global ICT community prepares to take a technological leap into IoT and 5G. Based on CTIA's experience, several core principles must be the touchstone of any future federal efforts.

A. Public-Private Partnerships Are The Bedrock Of Cybersecurity Policy.

CTIA supports the Commission's commitment to studying methods to "develop partnerships with industry, civil society, and international stakeholders."[105] As explained above, many partnerships are advancing cybersecurity, in the private sector, in international standards groups, emerging ISAOs and ISACs, and at DHS, NIST, and the FCC. Small and medium sized companies in sectors other than critical infrastructure are exploring their next steps to adopt a proactive cybersecurity posture. This is the time to nurture partnerships and support information sharing best practices that improve cybersecurity. The government should avoid undermining these efforts, and eschew a reactive, compliance mindset.

---

[103] U.S. GAO, INFORMATION SECURITY: BETTER IMPLEMENTATION OF CONTROLS FOR MOBILE DEVICES SHOULD BE ENCOURAGED, 35 (Sept. 2012), *available at* http://www.gao.gov/assets/650/648519.pdf.

[104] NTTAA, P.L. 104-113; OMB A-119, at 14, 17, *available at* https://www.whitehouse.gov/sites/default/files/omb/inforeg/revised_circular_a-119_as_of_1_22.pdf.

[105] *Commission Charter*, § 3.

B. The Government Should Exercise Regulatory Humility.

The RFI's interest in the proper role of government is critical and relates to every aspect of cybersecurity.[106] Existing, non-regulatory partnerships are effective because the private sector is best-positioned to develop technology solutions. As a result, the federal government should ask itself at every turn: will the contemplated activity—a regulation, information request, RFI, workshop—burden the private sector, undermine effective collaboration, or insert government where it need not be?

Several agencies have initiated proceedings, task forces working groups, and have solicited comment. NIST,[107] NTIA,[108] DHS,[109] FTC,[110] and FCC[111] all have efforts underway. Uncoordinated review could lead to disparate approaches, so the government should work to *consolidate* cybersecurity initiatives. Likewise, the government must recognize the burdens imposed on the private sector by duplicative efforts and inquiries. Multiplying agency requirements and responding to sometimes duplicative agency requests tax resources. It distracts companies from developing innovative, secure solutions.

C. Flexibility Is Key Because Threats And Responses Do Not Stand Still.

Global threats evolve rapidly, with attacks of varying sophistication coming from nation states, hacktivists, insiders, and terrorists. As CITA has explained in the context of mobile security, "[t]he cyberthreat landscape changes literally by the hour and requires constant vigilance and innovation throughout the entire U.S. [] industry."[112] And as FCC Chairman Wheeler noted, "[t]he pace of innovation on the Internet is much, much faster than the pace of a notice-and-comment rulemaking."[113] The private sector is succeeding in protecting consumers and continually responding to ever-changing threats, precisely because it is not saddled with outdated or onerous mandates. Rather than meeting arbitrary compliance obligations, it has the flexibility to use its expertise nimbly in response to security challenges.

D. The Government Should Promote Voluntary Standards and Technological Neutrality.

The government must avoid pushing particular standards or a one-size fits all approach. Economic literature is full of regulatory efforts that "foreclosed innovation, elected 'incorrect'

---

[106] *See* NIST RFI, 81 Fed. Reg. at 52828.
[107] *NIST Cybersecurity Framework*.
[108] NTIA, *Cybersecurity*, https://www.ntia.doc.gov/category/cybersecurity.
[109] DHS, *Cybersecurity*, https://www.dhs.gov/topic/cybersecurity.
[110] FTC, *Data Security*, https://www.ftc.gov/datasecurity.
[111] In its NPRM on broadband privacy, the FCC proposes rules on privacy and data security that promote a strict liability approach and may have the unintended consequence of limiting information sharing. *See* FCC, *Protecting the Privacy of Consumers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Rcd at 2540-41, ¶¶ 115, 117. *See also Use of Spectrum Bands Above 24 GHz for Mobile Radio Service*, Report and Order and FNPRM, 81 Fed. Reg. 58,270, FCC 16-89, ¶¶ 255-65 (rel. July 14, 2016) (proposing requirements for internet-connected device developers, including a network security plan).
[112] *CTIA White Paper on Mobile Security*, at 3.
[113] Remarks of FCC Chairman Tom Wheeler, American Enterprise Institute, at 4 (June 12, 2014), *available at* https://apps.gcc.gov/edocs_public/attachmatch/DOC-327591A1.pdf.

standards, or favored particular incumbent industries."[114] One recent example of conventional security wisdom changing involves passwords. Frequent changes were thought to be a sure-fire protection, but that theory is being reconsidered. Studies suggest that frequent changes may actually reduce security by encouraging users to adopt riskier passwords.[115] Another cautionary tale about locking in security approaches involves Domain Name System Security ("DNSSEC"). Early best practices identified DNSSEC in the late 1990s as a valuable tool to secure the DNS, but making it a requirement would have been unwise. Not only have technology and threats changed, DNSSEC may have unintended consequences, exacerbating other attacks, impacting reliability and cost, harming user experience, and burdening network capacity. Had policy makers required DNSSEC, innovation would have stalled and the DNS would be less secure. Thus, instead of regulation, the government should support voluntary, third party standards, which can be developed with broad input, adjusted over time, and used as appropriate.

E. Global Threats To The Internet And Communication Network Require The United States' Leadership.

Many threats originate from outside U.S. borders. Hacktivists, nation states, terrorists—each can and do exploit vulnerabilities in U.S. systems. In response to these global threats, industry has taken the lead. The mobile industry is heavily investing in new deployments like 5G and continues to develop security tools including firewalls, access control lists, intrusion detection and prevention, and security gateways. The government must lead international efforts to combat bad actors and improve security. The United States must support international efforts to address network-based threats to mobility, including device blacklisting and information exchange. The United States must champion U.S. innovation in global technology, eschewing regulation or international efforts that may skew competition. The United States must help global law enforcement and support the development of international norms. Without leadership and enforcement tools, borderless threats often cannot be mitigated until after harm is done. This may require revisiting mutual legal assistance treaties, and addressing difficult questions about law enforcement access to information stored in different jurisdictions.

F. Sensitive Vulnerability Information Can Be Exploited, And Must Be Treated With Great Care.

As we enter a new era of connectivity, entities with varied motives seek information about vulnerabilities. Researchers explore technologies and networks for flaws, raising questions about public disclosure and remediation in a complex ecosystem. Some unscrupulously seek and exploit vulnerabilities for profit.[116] The challenges surrounding public disclosure are receiving attention from industry, third party groups,[117] and government. Adding

---

[114] Michael G. Baumann & John M. Gale, *Economic Analysis of the Regulation of MVPD Navigation Devices* (2010).

[115] *See* Dan Goodin, *Frequent Password Changes are the Enemy of Security, FTC Technologist Says*, Ars Technica (Aug. 2, 2016), *available at* http://arstechnica.com/security/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says/.

[116] *See* J. Robertson, *Carson Block's Attack on St. Jude Reveals a New Front in Hacking for Profit* (Aug. 25, 2016), *available at* http://www.bloomberg.com/news/articles/2016-08-25/in-an-unorthodox-move-hacking-firm-teams-up-with-short-sellers.

[117] Some have challenged aspects of federal law that they claim limit research. *See* Complaint, *Green v. DOJ*, Civil Case No. 1:16-cv-01492 (D.D.C. filed July 21, 2016) (challenging the constitutionality of Section 1201 of the

to these complications, government also seeks information about threats and defenses.[118] Information about vulnerabilities, risk profile and system capabilities are unlike information traditionally collected by the government or shared among competitors. Public dissemination under regimes like FOIA risks competitive injury, but also can endanger security and help bad actors. Given the importance of transparency in government activity, agencies sometimes cannot guarantee protection of information from public disclosure. This is why ISACs and ISAOs are so vital; they facilitate sharing in a non-governmental setting, free from risk of inappropriate public disclosure. Information should not be lightly sought and should be treated with care.

G. User Education And Good Cyber Hygiene Are Critical.

No software, hardware or physical defense is impenetrable; end users have an enormous impact on security through inadvertence (*i.e.*, clicking on a phishing email) or conscious decisions (such a jailbreaking a phone or refusing to install an update). Combining education with good individual and organizational cyber hygiene will help immensely.[119] Ensuring a clean, healthy application ecosystem and consumer education are key to minimizing the effects of hackers and threats. Many incidents can be prevented or mitigated through basic steps to increase security, including readily available security tools, like passwords, PINs, and available two-factor authentication. It also is vital that consumers and organizations accept software and other updates for devices and systems. This country lacks a broad culture of cybersecurity awareness, but as detailed above, industry is successfully engaging the public on security.

H. The Government Must Work To Avoid Domestic and Global Fragmentation.

Federal law and policy require use of voluntary international standards, for good reason. The private sector can iterate technical solutions better and more quickly than any one government agency, particularly where the market is global in supply, demand, and interconnectedness. The United States must engage internationally and support standards to avoid fragmenting an inherently global market. Likewise, state efforts on cybersecurity are problematic. Not only is industry required to devote scarce time and resources to them, state-by-state requirements would balkanize approaches and solutions. The federal government should advocate existing cybersecurity policies, which rely on public-private partnerships and voluntary best practices, to promote a consistent approach.

Digital Millennium Copyright Act); Complaint, *Sandvig v. Lymch*, Civil Case No. 1:16-cv-01368 (D.D.C. filed June 29, 2016) (challenging the Computer Fraud and Abuse Act).

[118] *See, e.g.*, Press Release, *FCC Wireless Telecommunications Bureau Launches Inquiry into Mobile Device Security Updates* (May 9, 2016), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-339256A1.pdf (seeking information from wireless carriers on security updates for mobile devices); *Order to File a Special Report*, FTC Matter No. P165402 (May 9, 2016), *available at* https://www.ftc.gov/system/files/attachments/press-releases/ftc-study-mobile-device-industrys-security-update-practices/160509mobilesecuritymodelorder.pdf (ordering manufacturers to provide information on security updates for smartphones, tablets, and other mobile devices).

[119] *See CTIA White Paper on Industry Megatrends*.

By: /s/ Thomas C. Power

Thomas C. Power
Senior Vice President and General Counsel

Thomas K. Sawanobori
Senior Vice President, Chief Technology Officer

John M. Marinho
Vice President, Technology and Cybersecurity

CTIA
1400 16th Street, N.W., Suite 600
Washington, D.C. 20036
(202) 785-0081

September 9, 2016

APPENDIX
Select CTIA Publications and Filings on Cybersecurity

CTIA has been helping to develop flexible, voluntary, and effective cybersecurity in the mobile ecosystem. CTIA created its Cybersecurity Working Group ("CSWG"), which is comprised of senior technical and policy representatives from leading companies. CTIA's CSWG facilitates innovation and cooperation on advanced responses to evolving threats, as well as the formulation of policy positions and white papers in collaboration with government officials. CTIA has resources available for consumers, businesses and government. More can be found at http://www.ctialatest.org/category/cybersecurity-2/

CTIA White Papers. CTIA engages in research and thought leadership, offering the mobile industry's views on critical aspects of cybersecurity in several White Papers:

- *TODAY'S MOBILE CYBERSECURITY: INFORMATION SHARING* (Sept. 2014)[120]
- *MOBILE CYBERSECURITY AND THE INTERNET OF THINGS: EMPOWERING M2M COMMUNICATION* (May 2014)[121]
- *TODAY'S MOBILE CYBERSECURITY: INDUSTRY MEGATRENDS & CONSUMERS* (May 2013)[122]
- *TODAY'S MOBILE CYBERSECURITY: BLUEPRINT FOR THE FUTURE* (Feb. 2013)[123]
- *TODAY'S MOBILE CYBERSECURITY: PROTECTED, SECURED AND UNIFIED* (Oct. 2012)[124]

CTIA Comments on Cybersecurity. CTIA has actively participated in government efforts at DHS, FCC, FTC, GSA, and NIST on mobile and cybersecurity, including NIST's seminal work on the *Cybersecurity Framework*. CTIA's comments reflect the mobile sector's policy and technical perspectives. For example:

- Comments, *Views on the Framework for Improving Critical Infrastructure Cybersecurity*, NIST, Docket No. 151103999-5999-01 (Feb. 23, 2016)[125]
- Comments, *Experience with the Framework for Improving Critical Infrastructure Cybersecurity*, NIST, Docket No. 140721609-4609-01 (Oct. 10, 2014)[126]
- Comments, *Developing a Framework to Improve Critical Infrastructure Cybersecurity*, NIST, Docket No. 130909789-3789-01 (Dec. 13, 2013) (filed with National Cable & Telecommunications Association and US Telecom Association)[127]

---

[120] http://www.ctia.org/docs/default-source/default-document-library/ctia_informationsharing.pdf?sfvrsn=2
[121] http://www.ctia.org/docs/default-source/default-document-library/ctia-iot-white-paper.pdf
[122] http://www.ctia.org/docs/default-source/default-document-library/today-s-mobile-cybersecurity-industry-megatrends-amp-consumers.pdf?sfvrsn=0
[123] http://www.ctia.org/docs/default-source/default-document-library/cybersecurity_white_paper.pdf?sfvrsn=2
[124] http://files.ctia.org/pdf/CTIA_TodaysMobileCybersecurity.pdf
[125] http://csrc.nist.gov/cyberframework/rfi_comments_02_2016/20160223_CTIA-The_Wireless_Association.pdf
[126] http://csrc.nist.gov/cyberframework/rfi_comment_october_2014/20141010_ctia_marinho.pdf
[127] http://www.ctia.org/docs/default-source/Legislative-Activity/12-13-13-nist-comments-final-clean.pdf?sfvrsn=0