Before the Department of Homeland Security
Washington, D.C.

Request for Information	)	Solicitation Number:
	)	QTA00NS16SDI0003
Mobile Security Threats and Defenses	)	

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 Sixteenth Street, NW, Suite 600
Washington, DC 20036
(202) 785-0081
www.ctia.org

August 22, 2016

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

CTIA[1] submits this response to the Request for Information ("RFI") on Mobile Security Threats and Defenses issued by the Department of Homeland Security ("DHS"), with assistance from the Enterprise Mobility Program at the General Services Administration ("GSA").[2] Wireless is transforming government. From the way in which the government processes and collects data to the way in which it interacts with the public, mobility is being integrated into government functions. Given security threats to government networks and data, the government properly is looking at mobile security as part of its overall digital strategy.

The ecosystem supporting federal mobility is complex, extending beyond conventional IT elements to include OS providers, original equipment manufacturers ("OEMs"), application developers, enterprise solution providers, network operators and over-the-top ("OTT") security solution providers. Security in the ecosystem is rapidly changing along with the underlying technology. Industry groups have evolved 2G to 3G to 4G with increasing security, and are aggressively building security into the next generation of wireless, 5G. Device and network complexity have exploded since the advent of mobile voice service. As innovation progresses, the private sector is advancing mobile security faster than any agency could.

- Security is a top industry priority. Industry is making significant investments, and the entire ecosystem works tirelessly to innovate and advance security.
- As wireless becomes more pervasive through 5G and the Internet of Things, new approaches will emerge as industry aggressively innovates for security. Technology must advance at a very rapid pace—Internet speed—to address threats. Security needs often outpace standards bodies, as companies must monitor, protect, diagnose, and fight potential cyberattacks in real time.
- Flexibility and vigilance are vital in a changing threat landscape. It is imperative that the U.S. avoid regulatory burdens, which fundamentally are unsuited to the dynamic global threat landscape. Industry leadership, innovation, and freedom from regulatory burdens are the key to 5G security.

The government must avoid demanding singular solutions that could fragment the market, and it should refrain from imposing regulations that promote a compliance mindset.

---

[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] This RFI responds to direction from Congress to DHS to report on federal mobility. CTIA responds to Part 2 of the RFI, and addresses many of the threats identified in Part 1 as relevant.

Instead, the government must do more to integrate a comprehensive, flexible mobile strategy into risk management, and support collaborative work already underway.

II. MOBILITY IS POISED TO TRANSFORM THE IMPORTANT WORK OF GOVERNMENT.

The government is being transformed by mobility. Currently, the government uses mobility in two ways: (1) as an enterprise, supporting its various management and organizational initiatives, and (2) as a citizen-oriented tool to improve access to its services.[3] Government agencies rely on mobile differently and face varied challenges. Opportunities from mobility will continue to expand as industry looks ahead to 5G and the Internet of Things ("IoT").

The government is a vital partner. In its role as an enterprise user, the government must mitigate mobile risks and manage responses. To secure government data and communications, the government must heed advice to address mobile management—including security.[4] This includes educating users and using good cyber hygiene.[5] In its role as a regulator, the government must support innovation and collaboration, not regulation.

III. RAPIDLY CHANGING MOBILE SECURITY CHALLENGES SHOULD BE ADDRESSED WITH COLLABORATION AND USER EDUCATION.

The mobile ecosystem is growing rapidly. As CTIA has explained, "the move from PC applications to mobile apps is having a dramatic effect on all aspects of the marketplace."[6] From 2011 to 2014, domestic economic value generated from wireless grew 34% to $194.8 billion; apps alone have grown from $10 billion to $36 billion in four years. Threats rapidly evolve, and they are "increasingly more sophisticated."[7] As Federal Communications Commission ("FCC")

---

[3] The White House's *Digital Government: Building a 21st Century Platform to Better Serve the American People*, made the GSA responsible for helping agencies increase mobile access. https://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.htm. The U.S. Government Accountability Office ("GAO") found that "mobile Internet users reportedly face a range of challenges accessing government services online" but that progress is being made. GAO-15-69, *Mobile Devices: Federal Agencies' Steps to Improve Mobile Access to Government Information and Services* at 1 (2014).

[4] *See* U.S. Gov't Accountability Office, GAO 11-43, *Information Security: Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk* (2010).

[5] *See id.* at 1 ("Most agencies were missing key elements related to wireless security in their security awareness training."); *see id.* at 17-24 (discussing recommended security approaches).

[6] *Today's Mobile Cybersecurity, Industry Megatrends & Consumers*, CTIA, at 9 (2013), http://files.ctia.org/pdf/CTIA_IndustryMegatrends_Consumers.pdf.

[7] *See, e.g., Enterprise Mobile Threat Report: The State of iOS and Android Security Threats to Enterprise Mobility*, Lookout, at 2 (2015), https://info.lookout.com/enterprise-mobile-threatreport.html (click "Why Lookout" to download the report). The rise of mobile computing has pushed sensitive corporate data far beyond the traditional, firewall protected perimeter, and mobile devices now represent an increasingly attractive attack surface." *Id.* at 8.

Chairman Wheeler noted, "[t]he pace of innovation on the Internet is much, much faster than the pace of a notice-and-comment rulemaking."[8] Security practices cannot be static.

First, collaboration is integral to security, as the success of the National Institute of Standards and Technology ("NIST") Cybersecurity Framework ("Framework") demonstrates.[9] Particularly in mobile, where threats rapidly change, effective efforts draw on private innovation, along with the work of the government and third party groups. This has worked, yielding a comparatively low U.S. mobile malware infection rate and a robust mobile economy.[10]

Private innovation is critical. Carriers, OEMs, third-party solutions, and OTT apps are innovating on cybersecurity and consumer solutions. Offerings abound in mobile device management ("MDM") and enterprise mobile management ("EMM"), as innovation continues in virtualization and other ways to build and secure mobile devices and systems. Industry works together to respond to challenges. For example, in response to an uptick in mobile device theft, network operators, device manufacturers, and OS companies made the "Smartphone Anti-Theft Voluntary Commitment" to protect new models of smartphones against unauthorized use if they are lost or stolen.[11]

Nonregulatory government groups also do important work. NIST continues to be an effective convener of the private sector and the government, not just developing the successful Framework,[12] but also mobile-specific guidance. Recently, CTIA has worked with NIST to improve *SP-1800-4, Mobile Device Security: Cloud and Hybrid Builds*. At the FCC, the Communications Security, Reliability, and Interoperability ("CSRIC") and the Technological Advisory Council ("TAC") recommend best practices for mobile security. The FCC's CSRIC III, IV, and V have addressed the communications sector's cybersecurity needs. In 2013, CSRIC III released *Consensus Cyber Security Controls*—a final report on security controls, including

---

[8] FCC Chairman Tom Wheeler, Remarks at the American Enterprise Institute, Center for Internet, Communications and Technology Policy, at 4 (June 12, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DOC-327591A1.pdf.

[9] NIST, *Background: Framework for Improving Critical Infrastructure Cybersecurity* (Aug. 20, 2016), http://www.nist.gov/cyberframework.

[10] The United States successfully mitigates mobile malware attacks. *See* Verizon, *2015 Data Breach Investigations Report*, at 19-20 (2015), 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.").

[11] *Smartphone Anti-Theft Voluntary Commitment*, CTIA, (2016), http://www.ctia.org/policy-initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment.

[12] Many of Framework processes apply to mobility: inventorying physical devices and systems; prioritizing resources; managing identities and credentials for devices and users; managing remote access; and including cybersecurity in human resources practices, like deprovisioning.

for mobile devices.[13] In its recommendations, the TAC noted that standardized solutions are more beneficial for bad actors than for mobile device users.[14]

Likewise, critical activity continues at DHS in the National Cybersecurity & Communications Integration Center ("NCCIC"), the National Security Telecommunications Advisory Committee ("NSTAC"), and in Information Sharing and Analysis Organizations ("ISAOs"). Collaboration between industry groups and government is vital, as legislation like the Cybersecurity Information Sharing Act of 2015 confirms.[15] Such nonregulatory efforts allow flexibility as technology changes. The government should build on this cybersecurity work.

International standards groups and industry organizations, which are committed to promoting mobile security, drive consensus solutions with global reach. For example, the 3rd Generation Partnership Project ("3GPP") is a collaboration of associations that maintains global telecom specifications, including those related to cyber.[16] The Alliance for Telecommunications Industry Solutions ("ATIS") is creating "an overall industry framework for addressing cybersecurity threats."[17] ATIS' Cybersecurity Ad Hoc group is "examining existing cybersecurity frameworks … and how best to apply them."[18] And the Messaging, Malware and Mobile Anti-Abuse Working Group (M^3AAWG) works to protect the "ubiquitous [mobile] platform as it comes under attack from malware and messaging abuse."[19] M^3AAWG partners with the Global Cyber Alliance to "push the security community to more quickly adopt concrete, quantifiable practices that can reduce online threats."[20]

Second, user education is critical. As the CSRIC has explained, mobile users must learn about "the importance of, and the methods for, installing and using a suite of protective measures (e.g., strong passwords, anti-virus software, firewalls, IDS, encryption) and update as available."[21] CTIA and industry promote education, which changes behavior. In a recent survey, CTIA found that 69 percent of wireless consumers use PINs/passwords on their smartphones, up 13 percent from 2015, and up 38 percent from the first survey in 2012; 51

---

[13] FCC CSRIC, Consensus Cyber Security Controls (2013), https://www.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG11_Report_March_%202013Final.pdf.

[14] FCC, Technology Advisory Council, Presentation on Final Report to the TAC Recommendations (2012), https://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting121012/TAC12-10-12FinalPresentation.pdf.

[15] Pub. L. No. 114-113, Division N, 129 Stat. 2242, 2936 (codified at 6 U.S.C. §§ 1501-1510).

[16] *Today's Mobile Cybersecurity: Protected, Secured and Unified*, CTIA, at 21, http://www.ctia.org/docs/default-source/default-documentlibrary/today-s-mobile-cybersecurity-protected-secured-and-unified.pdf?sfvrsn=0 ("*Protected, Secured and Unified Whitepaper*").

[17] *Advancing ICT Industry Transformation*, ATIS, http://atis.org/about/index.asp.

[18] *ATIS Overview: Advancing ICT Industry Transformation,* ATIS, at 3 (2016) www.atis.org/01_images/PDFs/ATISOverview2016.pdf.

[19] *Why M^3AAWG?*, M^3AAWG, https://www.m3aawg.org/about-m3aawg.

[20] *Global Cyber Alliance Joins Forces with M^3AAWG to Drive Industry Adoption of Cybersecurity Solutions,* M^3AAWG (May 4, 2016), www.maawg.com/news/rel-GCA-joins-forces-with-M3aawg-2016-05.

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

percent have built-in remote lock and erase software installed on their smartphones, up 42 percent from 2015, and up 31 percent from 2012.[22]

Education is vital for the government. The GAO agrees: "it is important that an appropriate level of awareness [be] achieved among consumers who use mobile devices on a regular basis."[23] Industry has implemented many critical steps, and the federal government should do the same. For example, the United States Computer Emergency Readiness Team ("US Cert") offers advice for non-technical users, such as how to identify a threat and protect mobile devices,[24] but OPM and other guidance should target end users and include a focus on mobility.

IV. PRIVATE INNOVATION OFFERS THE GOVERNMENT MANY TOOLS TO ADDRESS MOBILE SECURITY.

A. The Government Should Leverage Tools That Mitigate Threats From Applications, Operating Systems, Devices, Networks And The Enterprise.

The RFI asks what "should the Government pursue to ensure security and the interoperability for mobile devices is robust and mitigates threats from. . . Applications; Operating System/ Firmware/Software; Device[s]; Networks; [and]Mobile Enterprise." Mobile device security and interoperability are robust, mitigating threats in each vector. The government should be forward-leaning: leverage existing capabilities and research, promote information exchange, and comprehensively manage mobile as part of overall digital strategy.

1. Applications: The Government Can Take Steps to Address Risks.

The government is understandably concerned about application threats. Many RFI concerns relate to malware, misuse, or unauthorized application access to data, surveillance, and ransomware. Related concerns implicate application store curation. These threats present challenges to the government as a purchaser and manager of mobile devices.

There is no one solution for application security; it relies on multiple layers of the mobile ecosystem. Major OS providers work with application developers on application security, and many OS application stores do a good job of screening for bad apps.[25] Network operators monitor traffic and combat threats. There are tools for consumers to address risks from apps that seek access to data or alter the function or security of the device.[26] There are also tools for

---

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

[23] U.S. Gov't Accountability Office, GAO-12-757, *Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged*, at 35 (Sept. 2012).

[24] U.S. Dep't of Homeland Security, U.S. Computer Readiness Team, *Tips*, https://www.us-cert.gov/ncas/tips.

[25] *See Protected, Secured and Unified Whitepaper*, at 11 (stores "vet apps so they do not contain malware.").

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

enterprise application management. One example of the layers coming together is the newly established AppConfig Community. In 2016, EMM solution providers formed it to "streamline the adoption and deployment of mobile enterprise applications by providing a standard approach to app configuration and management."[27] The effort aims to "mak[e] it simpler for developers to implement a consistent set of controls so that enterprise IT administrators can easily configure and manage apps according to their business policies and requirements."[28]

With other layers of the mobile ecosystem, the government can help address application-related threats. The government's role will depend on context, as it—like other enterprises—can act as a manager of mobility or its own developer. ***First***, as a manager of mobility, the government can encourage users to practice good cyber hygiene to avoid app-based problems. This includes keeping operating system and software up-to-date, only downloading apps from trusted stores, and not modifying devices. The government also must aggressively manage mobile devices and users: vet apps, limit downloads, and where appropriate, utilize tools, such as MDM capabilities that scan devices.

Second, where the government develops or desires its own applications—much less its own application store—it faces different challenges,[29] as discussed below. The government must pursue security by design, using best practices in app development with the support of trusted partners. The Federal Trade Commission ("FTC") has published tips to help developers incorporate security in development. While the FTC correctly makes clear that "[t]here is no checklist for securing all apps," and that it "doesn't prescribe a one-size-fits-all approach," these tips are a good starting point.[30] App store curation and management is even more complex, counseling in favor of careful government partnerships with qualified experts.

The government rightly assesses application security, because cyber threats can jeopardize the public sector as well as the private sector.[31] For example, threats like ransomware

---

[27] *What is the AppConfig Community?*, AppConfig Community, www.appconfig.org/about.
[28] *Id.*
[29] *See* The White House, *Agency Mobile Apps/Mobile Sites*, https://www.whitehouse.gov/digitalgov/mobile (listing examples of agency efforts). Some government apps are available in major app stores. *See, e.g., iTunes Store*, Application by U.S. Gov't Accountability Office, https://itunes.apple.com/us/app/gao/id489666309?mt=8.
[30] FTC, *Mobile App Developers: Start with Security* (February 2013), www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security.
[31] For example, using stolen passwords and logins, hackers broke into the Office of Personnel Management ("OPM") databases in 2014, exposing the sensitive information of 22.1 million people. *See* E. Nakashima, *Hacks of OPM databases compromised 22.1 million people, federal authorities say*, Washington Post (July 9, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/. In a 2015 IRS attack, hackers "stole information from 330,000 taxpayers to successfully file bogus tax refunds and obtain $50 million in federal funds." Jonathan Chew, *The IRS Says Identity Thieves Hacked Its Systems Again*, Fortune (Feb. 10, 2016), http://fortune.com/2016/02/10/irs-hack-refund/. *See* GAO 11-43, *supra* note 4, at 1 (mobility "provide[s] many potential benefits, including greater flexibility for a mobile workforce and ease

are not unique to the private sector or government. Since June 2015, the NCCIC has initiated or received 321 reports of ransomware-related activity affecting 29 different federal agencies.[32] The government can prepare for and protect against threats by taking appropriate measures, such as backing up data, segmenting networks and data, and having a response plan.

2. OS/Firmware/Software: Security Requires The Entire Ecosystem.

DHS's identified concerns include the update process for OS, firmware, and software. The update process is complex and varies across operating systems, manufacturers, carriers and applications. Updates rely on OS providers, OEMs, carriers, and end users. There is variety in vulnerabilities, their severity, and solutions, so the update process must manage and mitigate risk.[33] The FTC and FCC are looking at mobile device security and the update process.[34] NIST is working on mobile security,[35] as is the National Telecommunications and Information Administration ("NTIA"), particularly in the Internet of Things ("IoT").[36]

The government can take steps as a consumer to address OS/Firmware/Software risks. For example the government and its users receive updates to mobile OS and apps. Government must encourage a culture of security, including accepting updates. There are challenges in government mobile and bring your own device ("BYOD") management, with employees using and storing work info on private devices, downloading apps on government devices through third parties, and jailbreaking devices. The government must combat these bad habits.

3. Devices: Many Physical Risks Can Be Addressed With Better Education And Prevention.

---

of installation and use, they also pose significant risks to information and systems" across the government).

[32] *See* U.S. Dep't of Homeland Security, *Response to Senators Carper and Johnson's Dec. 3, 2015 Letter,* at 6 (2016) report, https://www.hsgac.senate.gov/media/minority-media/dhs-doj-respond-to-carper-inquiries-on-agencies-response-to-threat-of-ransomware.

[33] Verizon explains, "sometimes you just can't fix a vulnerability—be it because of a business process, a lack of a patch, or incompatibilities…. It's important to realize that mitigation is often just as useful as remediation—and sometimes it's your only option." Verizon, 2016 Data Breach Investigations Report, at 16 (2016).

[34] The FTC held a workshop in 2013 and in 2014, it sought comment on mobile device security, including secure platform design, distribution channels, development, and security updates. *See* Press Release, FTC, *FTC Invites Further Public Comment on Mobile Security* (April 17, 2014), https://www.ftc.gov/news-events/press-releases/2014/04/ftc-invites-further-public-comment-mobile-security. The FTC and FCC have launched an inquiry into security updates. *See* Press Release, FTC, *FTC to Study Mobile Device Industry's Security Update Practices* (May 9, 2016), https://www.ftc.gov/news-events/press-releases/2016/05/ftc-study-mobile-device-industrys-security-update-practices.

[35] *See* NIST/NCCOE, 1800-4, *Mobile Device Security, Cloud and Hybrid Builds* (2015) (Draft); NIST 800-124 *Revision 1 (final), Guidelines for Managing the Security of Mobile Devices in the Enterprise* (2013); NIST 800-163 *Vetting the Security of Mobile Applications* (2015).

[36] https://www.ntia.doc.gov/federal-register-notice/2016/rfc-potential-roles-government-fostering-advancement-internet-of-things.

As the government considers device-based threats, it is important to remember that hardware-based security and robust MDM are important, but they are not a panacea. End user awareness is key, as even the most "secure" devices can be put at risk by user habits, such as choosing not to use passwords (or to use weak ones), downloading apps from insecure sites, or using devices on unsecured networks. Some of RFI's identified threats, such as data loss from stolen devices, can be mitigated by software and design innovation, but others are outside the control of operators, OEMs and developers.

Industry has been leading on both fronts—hardware- and software-based security and consumer education. Regarding hardware and software, industry has been aggressive. One example is the "Smartphone Anti-Theft Voluntary Commitment," an effort by CTIA and the wireless industry to deter smart phone thefts. This voluntary commitment calls for a baseline anti-theft tool to be included on wireless smartphones.[37] In general, industry has been building additional layers of increasing complexity for device authentication and authorization. For example, SIM cards now are securely loaded with authentication keys for devices and networks. As for consumer-based security, industry is continuing to educate consumers about passwords, apps, and capabilities to secure devices.

Like the private industry, the government can address risks using hardware-and software-based solutions along with the end-user focused solutions. It can also support review and research into roots of trust and related approaches, such as TrustZone from ARM. The government should not become dependent on one solution—such as hardware roots of trust—because the ecosystem is developing varied complementary approaches to mobile security.

Additionally, the RFI asks about "supply chain manipulation." As CTIA explained to GSA,[38] global mobile supply chains are complex. Among other things, there are differences in software and hardware sourcing. Industry promotes best practices, pushing standards down and using trusted partners. The government should look to best practices in hardware and software sourcing. For instance, 3GPP SA Working Group 3 identifies security assurance methodologies for 3GPP network elements.[39] In addition, ISO/IEC 15408, the Common Criteria for Information Technology Security Evaluation, and the internationally-recognized Common Criteria Recognition Agreement ensure that products can be evaluated by competent, independent labs and certified to meet security properties.[40] In addressing supply chain risks, the government should avoid inadvertently pursuing policies that could be seen as protectionist.

---

[37] *See Smartphone Anti-Theft Voluntary Commitment*, CTIA, *supra* note 11.

[38] *Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition*, CTIA, Comments Before the Office of Emergency Response and Recovery of the GSA (June 7, 2013), http://files.ctia.org/pdf/GSA_CTIA_Comments_June7th_2013.pdf.

[39] *See* 3GPP, *Draft Meeting Report for TSG SA WG3 Meeting S3#70*, at § 8.3 (Jan. 21, 2013), https://www.google.com/url?q=http://www.3gpp.org/ftp/tsg_sa/wg3_security/TSGS3_70_Sophia/Report/MeetingReport_SA3%252370.doc&sa=U&ved=0ahUKEwja9Zv4mdXOAhVG0h4KHTDqB_8QFggEMAA&client=internal-uds-cse&usg=AFQjCNGnHH96sBBl-OGmaUT1k0-UjSjVqA.

[40] Common Criteria, Home Page, http://www.commoncriteriaportal.org/.

4. Network: Complex Threats Require Global Action, Not Solely Technical Solutions, Particularly As Networks Evolve.

Many threats extend beyond the device and are fundamentally about wireless networks and internet security. Threats come from global actors, such as hacktivists, nation states, and terrorists, particularly when the system of trust relied upon by operators and ISPs erodes. Network security cannot be achieved through technology and education alone, and the government should be wary of trying to use device security to address network security risk. Procurement expectations or mobile management will not be enough.

Industry is leading on network security, particularly as it migrates to 5G, which will be the backbone for billions of connected devices globally. Operators constantly develop new ways to manage risk using a layered approach that lets them adjust as threats change. Industry has a range of network security tools, such as firewalls, access control lists, intrusion detection and prevention, and security gateways. Anticipating 5G and the Internet of Things, industry is putting in place improved encryption and security protocols responsive to anticipated use scenarios, distributed and secure network architecture, decentralized, flexible and adaptive security approaches, diversity in network architecture and functions, and enhanced device security across the variety of anticipated device types. In addition, operators are working internationally on efforts like blacklisting databases, which would benefit from additional participation.

To support these efforts, and the development of new platforms and deployments like 5G, numerous standards are regularly in flux. While this can be challenging to the private sector and confusing to government, it allows flexibility for industry to customize what works for each element. The government should resist the urge to standardize best practices through procurement policy. Instead, it should allow security companies—the true experts—to address evolving threats as networks and solutions change over time.

To be sure, the government can help. ***First***, the government should support international efforts to address network-based cyber threats impacting mobility. Examples include device blacklisting, and improving information exchange between countries. ***Second***, the government should champion U.S. innovation and leadership in global technology, eschewing regulation that may skew interoperability and competition as innovative networks mature. ***Third***, the government should help law enforcement agencies and their representatives respond to borderless threats. ***Fourth***, the government should provide international leadership to combat global cyber threats by championing international rules and methods to bring criminals to justice. Without leadership and legal enforcement tools, foreign threats often cannot be mitigated until after measureable harm is already done.

5. Enterprise: Government Mobile Enterprise Risks Can Be Mitigated With Existing Best Practices, Tools, And Aggressive Management.

The two mobile enterprise threats identified in the RFI are complex.[41] The first focuses on security breaches of systems that support mobility. Exploitation of enterprise mobility management and mobile device management systems or obtaining administrator credentials is often the result of social engineering attacks, insider threats, and human error/poor hygiene. The second threat identified in the RFI relates to private enterprise mobile app stores. This implicates credentials compromise as well as compromised application development that permits bad apps to be posted in app stores.

In considering the first threat, the government can help mitigate threats exploitation of MDM systems and obtaining administrator credentials. The first step is to develop and execute a comprehensive digital security strategy that includes common sense management of mobile in the enterprise. Whether the government uses MDM or EMM solutions, a digital security strategy will involve inventorying assets, disabling unused devices and services, removing unused accounts, restricting application downloads where appropriate, applying the latest patches, and closing open and unused ports, to name a few. Securing privileged credentials also is important, and more needs to be done in the private sector[42] and in government to use best practices, including appropriate encryption, authentication, frequent changes and segmentation.[43]

Broadly speaking, there is no one way to securely manage enterprise mobility. Innovation continues, with debate around hypervisors and containerization, antivirus applications, trusted execution environments, authentication methods, mobile application management and mobile information management. It would be a mistake to promote particular approaches, because conventional wisdom about security changes.[44] The government's approach must be realistic, technologically neutral, and supportive of private sector innovation. It also must be flexible because the government sources from a diverse marketplace (the master schedule has numerous carriers and manufacturers, as well as MDM providers), supports BYOD, and has a multiplicity of agencies and missions. Enterprise needs vary across missions and small enterprises have different needs compared to those that are larger.

---

[41] The identified threats are: (1) "Exploitation of Enterprise Mobility Management/Mobile Device Management systems or obtaining administrator credentials" and (2) "Exploitation of private enterprise mobile application stores, including obtaining administrator credentials or methods of subverting application security vetting procedures."

[42] In a recent survey of corporate CIOs, "83 percent of respondents face numerous challenges with managed privileged accounts and administrative passwords." Thor Olasrud, *Organizations Sloppy About Securing Privileged Accounts,* CIO (Nov. 17, 2015, 6:54 AM PT), http://www.cio.com/article/3005613/security/organizations-sloppy-about-securing-privileged-accounts.html.

[43] *See, e.g.*, Harish Setty, *System Administrator - Security Best Practices* (2001), SANS Institute InfoSec Reading Room, https://www.sans.org/reading-room/whitepapers/bestprac/system-administrator-security-practices-657; Yuri Diogenes, Microsoft blog post, *Securing Privileged Access,* Microsoft (June 3, 2016), https://technet.microsoft.com/windows-server-docs/security/securing-privileged-access/securing-privileged-access.

[44] *See* Dan Goodin, *Frequent Password Changes are the Enemy of Security, FTC Technologist Says*, ARS Technica (Aug. 2, 2016, 5:51 PM), http://arstechnica.com/security/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says (recounting comments of FTC Chief Technologist on wisdom (or lack thereof) of frequent password changes).

Fundamentally, agencies should use the NIST Cybersecurity Framework and the NIST Risk Management Framework to prioritize. The NIST Cybersecurity Framework contains a voluntary, risk-based management process to assess security risks.[45] It can help manage enterprise mobility. Likewise, the NIST Risk Management Framework provides guidelines for security controls in government information systems.[46] Both should be foundational elements of agencies' digital strategy. These frameworks are useful because they are the result of collaboration between industry and government.[47] NIST produces guidance for federal systems, ranging from hardware expectations to authentication protocols.[48] The government must support these collaborations, which yield informed, flexible guidance.

As for the second threat identified—app store compromise—government must take a broad view, recognizing its own limitations. Federal efforts on app and app store development have had limited success, as sometimes app store creation and management are outsourced poorly. Private app store curation requires vigilance and cooperation between the developers and enterprise. CTIA recommends using trusted sourcing partners for applications, requiring security by design, including secure systems in the device design life cycle, and enforcing best practices for IT system management to support mobility in the enterprise.

B. Industry Is Addressing The Critical Points In The Communication Chain As Networks Mature And Turn to 5G.

Part 2 of the RFI inquires, "What are the demarcation points on a mobile communication chain that need attention and are not already covered by industry?" Efforts across the ecosystem address security throughout the communication chain. In terms of the network and critical points and functions, the FCC's CSRIC IV Working Group mapped the NIST Framework onto the wireless segment, and identified critical areas of focus, which industry is addressing: location registers, identity and authentication registers, mobile switching and packet core entities, mobility management core entity, core signaling entities, core policy entities.[49] As industry looks to 5G and IoT, efforts on security have intensified, and standards bodies here and abroad are building in aggressive and flexible security approaches. Security for 5G must be nimble, iterative and comprehensive as uses develop.

That said, there are risks in a truly global, connected communications and internet infrastructure, particularly where U.S. networks interact with those around the world, sometimes

---

[45] NIST, 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems* (2010); NIST, *Cybersecurity Framework—Workshops and Events* (updated June 9, 2016), http://www.nist.gov/cyberframework/cybersecurity-framework-events.cfm.
[46] NIST, 800-37, *supra* note 45.
[47] The government should encourage stability in these foundational documents.
[48] *See, e.g.*, Draft NISTIR 8011 Vol. 2, *Automation Support for Security Control Assessments* (2016) (providing guidance on managing security concerns related to unmanaged devices in information systems); Draft NIST 800-63B, *Digital Authentication Guideline* (2016)(providing technical guidance on authentication for remote digital interaction).
[49] *See* CSRIC Council IV, *Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report*, 128 -129 (2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

operated by foreign entities, some of whom who may abuse opportunities. Some security solutions depend on widespread or universal adoption, which may not be possible now. As mutual trust in those connections and between interconnected operators is challenged, the ecosystem must adjust; this includes government, which should lead internationally in encouraging collaboration and mitigation, and redoubling efforts to hold bad actors accountable.

C. DHS Should Support Global Standards To Avoid Fragmentation, And Help Stop Emerging Regulatory Overreach.[50]

Many agencies are looking at mobile security, considering regulations and approaches, and seeking information. Multiplying agency requirements and duplicative agency inquiries tax private resources and distract companies from their core missions: developing innovative, secure solutions and advancing effective cybersecurity. To avoid adding another regulatory layer, the government should evaluate efforts and standards already in place.

Currently, multiple agencies have initiated proceedings, case studies, task forces, or working groups to review cybersecurity regulations and have requested that the private sector provide input. In the executive branch, the FTC,[51] FCC,[52] NIST,[53] and NTIA[54] are examining cybersecurity, in particular mobile security, in different ways. In fact, some agencies, like the FCC, have multiple cyber efforts in place at the same time. DHS continues its productive efforts in several venues. Various states also look at mobile security risks and threats. For example, the 2015 California Kill Switch law[55] requires that all smartphones sold in the state come with "kill switch" software; some states, like Connecticut, have initiated proposals on cybersecurity.[56]

Duplicative government efforts burden companies across the ecosystem. Their cyber leadership must manage demands for information, and respond to policy proposals while

---

[50] The RFI asks (questions 3 and 4) "Are there any standards not being implemented today that should be leveraged to improve mobile security?" and "Are there any standards that have stalled or should be started that could be leveraged to improve security?" CTIA answers these together.

[51] *Data Security*, FTC, https://www.ftc.gov/datasecurity.

[52] *Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security*, FCC (Tuesday, November 17, 2015), https://www.fcc.gov/public-safety/cybersecurity-and-communications-reliability-division-public-safety-and-homeland; *Cyber Security and Network Reliability*, FCC, https://www.fcc.gov/general/cyber-security-and-network-reliability; *Communications Security, Reliability, and Interoperability Council V*, FCC (Wednesday, July 20, 2016), https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability#block-menu-block-4.

[53] *Latest Update*, NIST (updated Aug. 20, 2016) http://www.nist.gov/cyberframework/.

[54] *Multistakeholder Process: Cybersecurity Vulnerabilities*, NTIA (April 08, 2016), https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilitiesU.

[55] S.B. 962, 2013-2014 Leg. (Ca. 2014).

[56] State of Connecticut Public Utilities Regulatory Authority, 14-05-12, *Connecticut Public Utilities Cybersecurity Action Plan* (2016) http://portal.ct.gov/uploadedFiles/Departments_and_Agencies/Office_of_the_Governor/Press_Room/Press_Releases/2016/04-2016/2016.04.06%20Connecticut%20Public%20Utilities%20Cybersecurity%20Action%20Plan.pdf.

maintaining partnerships that have been the hallmark of effective cybersecurity. In addition to diverting resources from security, diffuse government efforts and inquiries raise concerns about preserving the confidentiality of information about risks, mitigations, preparedness, and strategy, which the private sector does not want bad actors or third parties to obtain.

As standards develop, expectations must remain voluntary and not become de facto regulation or overbroad procurement standards. The government should resist encouraging particular standards that will limit industry innovation, and should help industry advocate internationally for flexible, open standards that do not prematurely lock in one approach. DHS and GSA should promote voluntary third party standards and innovation, consistent with the National Technology Transfer and Advancement Act of 1995 ("NTTA") and OMB Circular A-119, which require reliance on the private sector to lead standardization.[57]

V. IN CONCLUSION, SEVERAL PRINCIPLES MUST INFORM GOVERNMENT CONSIDERATION OF MOBILE SECURITY.

In light of the forgoing, the government should be guided by several principles to protect the mobile ecosystem and ensure the private sector and government benefit from standards that are effective, non-duplicative and flexible.

- Public-private partnerships have been the bedrock of cybersecurity innovation and policy. No federal agency should undermine effective collaboration by pursuing regulation, or burden the private sector with duplicative initiatives.

- Neither threats nor solutions stand still. Conventional wisdom about best practices can change, so the government should be vigilant to avoid prematurely locking in solutions.

- Threats are global, demanding government help to secure networks and defeat attacks.

- Cyber risk information must be treated with care. Collecting and making public detailed information about threats and defenses threatens to undermine security. A gap analysis may help bad actors, as will a matrix mapping threats and tactics to defenses.

[57] To reduce costs, provide incentives to serve national needs and encourage trade, competition, and private expertise, the NTTA requires that "all federal agencies must use voluntary consensus standards in lieu of government-unique standards in their procurement and regulatory activities, except where inconsistent with law or otherwise impractical." The White House, Circular No. A-119 Revised (1999), https://www.whitehouse.gov/omb/circulars_a119. This reflects confidence in "[t]he vibrancy and effectiveness of the U.S. standards system in enabling innovation." The White House Memorandum from Aneesh Chpora, Miriam Sapiro, and Cass Sunstein, to the Heads of Executive Departments and Agencies, *Principles for Federal Engagement in Standards Activities to Address National Priorities* (January 17, 2012) https://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-08_1.pdf; *see also* Exec. Order 13718, 81 Fed. Reg. 7441, 7443 (2016).

- Mobility is a part of overall information technology and data security strategy. MDM, EMM, MAM, virtualization, and other capabilities, while not a panacea, are vital tools that can help the government—like other enterprises—manage mobility.

- End users are critical. Combining education with organizational cyber hygiene can help address many of the threats identified in the RFI.

- The government should maintain technological neutrality. The federal government is not supposed to pick winners and losers and should avoid a one-size fits all approach.

- The government should avoid inadvertently fragmenting a global market. Federal law and policy require use of voluntary international standards, to promote interoperability and economies of scale. DHS should avoid U.S.-specific standards, particularly while industry is addressing security through standards groups that enable global roaming.

The federal government as a user and beneficiary of mobility can promote innovation and avoid unnecessary regulation and duplication of effort. CTIA looks forward to helping DHS address federal mobile device security.

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 Sixteenth Street, NW, Suite 600
Washington, DC 20036
(202) 785-0081
www.ctia.org

August 22, 2016