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

Request for Comments	)	
	)	
Draft Interagency Report on Status	)	Draft NISTIR 8200
Of International Cybersecurity	)	
Standardization for the Internet of Things	)	
	)	

COMMENTS OF CTIA

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

April 18, 2018

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY

CTIA[1] appreciates the opportunity to comment on the National Institute of Standards and Technology ("NIST") Draft Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things ("Draft NISTIR 8200" or "Draft Report").[2] Cybersecurity, including for the Internet of Things ("IoT"), is one of CTIA's top priorities. CTIA applauds NIST's support for Standards Developing Organizations ("SDOs"), because the "[e]stablishment and use of international cybersecurity standards are essential for: improving trust in online transactions, mitigating the effects of cyber incidents (e.g., crime), and ensuring secure interoperability among trade partners, thereby facilitating increased efficiencies in the global economy."[3]

CTIA offers a few clarifications. For example, although it is reasonable to describe standards in terms of maturity,[4] NIST's conclusions about lagging adoption may be misplaced.[5] This is particularly true in the discussion of network security.[6] NIST should emphasize the voluntary nature of the identified standards and refine its use cases to focus on the federal government. CTIA encourages NIST to engage more closely with stakeholders and coordinate federal efforts in SDO-led initiatives. NIST should also feature its own successful guidelines like the NIST *Framework for Improving Critical Infrastructure Cybersecurity* ("*Cybersecurity Framework*").[7]

II. NIST IS RIGHT TO PROMOTE FEDERAL PARTICIPATION IN INTERNATIONAL STANDARDS WORK.

NIST is correct that "[t]he availability and use of international cybersecurity standards are major factors for ensuring the secure and resilient operation of the expanding number of

---

1 CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

2 Draft NISTIR 8200, Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT) (Feb. 2018) ("Draft NISTIR 8200").

3 Draft NISTIR 8074 (Volume 2), Supplemental Information for the Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity, at 2 (Aug. 2015).

4 *See* Draft NISTIR 8200, at 61, Annex C, Table 6.

5 *See id.*, at 53-54, Table 4.

6 *Id.*, at 54.

7 NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (Feb. 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf. *See also* NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, *Draft Version 1.1* (Jan. 10, 2017), https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf.

agency mission critical IoT systems."[8] International, industry-led standards bodies are working on standards to facilitate IoT security and promote open markets with free cross-border data flows, economies of scale, and interoperability.

The government's adoption of consensus-based international standards can set an example. Last fall, the Department of Homeland Security ("DHS") directed agencies to implement Domain-based Message Authentication Reporting and Conformance ("DMARC")—a protocol created by industry and developed by the Internet Engineering Task Force ("IETF") to combat phishing and other fraudulent emails.[9] Studies show that organizations using DMARC receive 23% fewer email threats.[10] Government adoption of international standards can have a positive spillover effect through risk-based procurement strategy.[11]

NIST should "coordinate U.S. government participation in international cybersecurity standardization for IoT."[12] Speaking with one voice is important to promote free markets and maintain U.S. leadership. NIST's involvement in the development of voluntary standards for Smart Grids illustrates the agency's ability to convene key stakeholders, including foreign governments. NIST devoted considerable resources to bilateral and multilateral engagement on the development of international Smart Grid standards.[13] With the International Trade Administration and Department of Energy, NIST established the International Smart Grid Action Network—a multinational organization comprised of 23 countries and the European Union—to complement efforts by the global stakeholder organization Global Smart Grid Federation.[14] NIST continues to work with international stakeholders to harmonize evolving Smart Grid architectures.[15]

NIST is uniquely qualified to encourage international collaboration on global security. The American National Standards Institute ("ANSI") has emphasized that the strength of the United States' public-private partnerships is unparalleled because they are true partnerships: "Neither government nor industry claims or exerts overall authority over the other, and by working together in respectful cooperation, we are able to most effectively respond to the

---

[8] Draft NISTIR 8200, at 56.

[9] Department of Homeland Security, Binding Operational Directive 18-01 (Oct. 16, 2017), https://cyber.dhs.gov/bod/18-01/.

[10] GreatHorn, *GreatHorn's 2017 Spear Phishing Report Shows that 91 Percent of Phishing Attacks are Display Name Spoofs* (Jan. 31, 2017), https://www.greathorn.com/greathorns-2017-spear-phishing-report-shows-91-percent-phishing-attacks-display-name-spoofs/.

[11] *See* Draft NISTIR 8200, at 56 ("In accordance with USG policy, agencies should participate in the development of these standards in many SDOs and, based upon each agency's mission, cite appropriate standards in agency procurements.").

[12] Draft NISTIR 8200, at ii.

[13] *See* NIST SP 1108R2, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2, at 33-34 (Feb. 2012); NIST SP 1108R3, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3, at 33-35 (Sept. 2014).

[14] *Id.*, at 34.

[15] *See* NIST SP 1108R3, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3, at 35-36 (Sept. 2014).

strategic needs of the nation."[16] NIST should lead by example and encourage other countries to engage in standards-development efforts instead of government mandates.

III. THE DRAFT TAKES THE RIGHT APPROACH, BUT SHOULD CLARIFY A FEW KEY AREAS, SUCH AS FEATURING THE CYBERSECURITY FRAMEWORK AND EMPHASIZING AREAS RELATED TO THE VOLUNTARY NATURE OF STANDARDS, CONNECTED VEHICLES, AND A FEDERAL GOVERNMENT FOCUS.

Draft NISTIR 8200 strives to offer a wholistic view of IoT security. The Report describes five IoT technology application areas—vehicles, consumer IoT, health IoT and medical devices, smart buildings, and smart manufacturing—and provides examples of relevant standards for eleven core areas. This is laudable, but CTIA recommends that NIST clarify the voluntary nature of the standards and refine its discussion of adoption.

A. NISTIR 8200 should feature the *Cybersecurity Framework* and other NIST work.

NIST does excellent work leading the creation of consensus-based approaches like the *Cybersecurity Framework*. It is puzzling that Draft NISTIR 8200 does not refer to them or urge their use, particularly now that use of the *Cybersecurity Framework* is mandatory for federal agencies. Doing so would also help the international community, which looks to NIST's products to inform further work. The *Cybersecurity Framework* has influenced cybersecurity in the U.S. and abroad. NIST should emphasize the characteristics that made it a success: its "voluntary, risk-based, prioritized, flexible, repeatable, and cost-effective approach."[17]

The Draft Report also should address other NIST guidance, industry activities, and public-private partnerships. The U.S. Chamber of Commerce, for example, published a whitepaper identifying key principles for IoT security.[18] CISCO has circulated a draft framework for securing IoT, which focuses on the characteristics of IoT and Machine-to-Machine communications.[19] Guidance from groups like the National Security Telecommunications Advisory Committee ("NSTAC") or the Federal Communications Commission's ("FCC") Communications Security Reliability and Interoperability Council ("CSRIC") and Technological Advisory Council ("TAC") have generated useful work.

---

[16] ANSI Response to Request for Information, NIST, Effectiveness of Federal Agency Participation in Standardization in Select Technology Sectors for National Science and Technology's Council's Sub-Committee on Standardization, Docket No. 0909100442-0563-02, at 1 (filed Mar. 4, 2011), *available at* https://www.nist.gov/sites/default/files/documents/standardsgov/ANSI-Response-to-Request-for-Information-on-Federal-Agencies-030411.pdf.

[17] Testimony of Charles H. Romine, Ph.D., Director, Information Technology Laboratory, NIST, before the United States House of Representatives, Committee on Science, Space, and Technology, Subcommittee on Research and Technology (Feb. 14, 2017).

[18] U.S. Chamber of Commerce and Wiley Rein LLP, *The IOT Revolution and Our Digital Security: Principles for IoT Security* (Sept. 2017), https://www.uschamber.com/IoT-security.

[19] CISCO, *Securing the Internet of Things: A Proposed Framework* (May 19, 2015), https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html; CISCO, *Securing the Internet of Everything* (2012), https://www.cisco.com/c/dam/en/us/products/collateral/security/holistic-approach.pdf.

B. The NISTIR should clarify that identified standards are voluntary.

The only prominent reference to the voluntary nature of identified standards is in the first sentence of Section 2 (Scope).[20] NIST should add language emphasizing that private use of standards is voluntary and that identification of standards does not constitute an endorsement. For example, Draft NISTIR 8200 cites International Organization for Standardization ("ISO") standards on vulnerability handling and disclosure.[21] Such programs are complex,[22] requiring organizations to scope the program, allocate resources, consider how they will resolve reports, and understand legal obligations to notify business partners, regulators, and the public. Vulnerability disclosure programs may not work for many organizations, particularly small businesses with limited resources.

NIST should emphasize the standards' voluntary nature in Sections 1 (Introduction) and 2 (Scope), the identification of relevant standards in Section 6 (Cybersecurity Areas and IoT), and the introduction of Appendix D (IoT Standards Mapping to Core Areas of Cybersecurity).

C. NIST should more accurately characterize the availability and uptake of standards by deleting or adjusting Table 4.

In several places the Draft Report states that there are market deficiencies and that standards are lacking. For example, NIST says that "market implementations" of cyber incident management are "lagging for IoT systems" just after concluding that identified incident management standards "have widespread market acceptance."[23] It is unclear what NIST believes is "lagging" or on what it bases this conclusion.

Table 4 (Status of Cybersecurity Standardization for Several IoT Applications) offers sweeping generalizations. NIST indicates that the table is based upon "the proceeding information and analysis," but none of the market impact statements in Section 8 (Standards Landscape for IoT Cybersecurity) provide sources supporting its conclusions. The Draft simply uses statements like, "Unknown," "Existing standards are being implemented," "Although standards exist, practical applications to IoT systems has not been consistently demonstrated," or "[t]he market has been slow to implement."[24] Not only does Table 4 lack support, it is confusing and presents an inaccurate picture. In almost every use case, it indicates that standards are needed and/or have not been implemented.[25] This may suggest to readers in governments around the world that there are no relevant standards, when SDOs like the 3rd Generation Partnership Project ("3GPP"), 3rd Generation Partnership Project 2 ("3GPP2"), International

---

[20] Draft NISTIR 8200, at 2.

[21] *See e.g., id.*, at 24, 30, and 48.

[22] *See* Megan L. Brown & Matthew J. Gardner, *Considering a Vulnerability Disclosure Program? Recent Push Raises Questions for General Counsel*, CircleID (Feb. 10, 2017), http://www.circleid.com/posts/20170210_considering_a_vulnerability_disclosure_program/.

[23] Draft NISTIR 8200, at 48.

[24] *See id.*, at 46-52.

[25] *See id.*, at 53-54.

Electrotechnical Commission ("IEC"), Internet Engineering Task Force ("IETF"), Institute of Electrical and Electronics Engineers ("IEEE"), ISO/IEC JTS1, ITU-T, the Open Group, WiMAX Forum, and others have been actively engaged. Standards and best practices exist and their adoption is on the rise. One survey revealed that 84% of organizations—varying in size and industry—have adopted some type of security framework, and that 44% of organizations use more than one.[26] CTIA recommends that NIST delete Table 4 or edit it to ensure that it reflects the current state of standards availability and adoption.

D. The discussion of network security and connected vehicles should be expanded.

NIST should broaden its discussion of network security. The current draft does not appear to recognize the different roles that SDOs play. Some, like IETF, create baseline standards that are used by 3GPP and others to build profiles for network security, while other SDOs may play a less fundamental role. Likewise, standards apply differently to parts of the network. There are layers to network security, from access control and intrusion prevention to security for applications and wireless networks. Some 3GPP standards are mandatory for certain network aspects, like the radio access network ("RAN"). Others are voluntary and allow for more flexible adoption. Additionally, some solutions are not adopted by end users, because of the age of their devices or a choice not to update. This is not clear in the Draft Report.

Communications networks evolve. Industry is developing standards to enhance security for deployment of 5G networks, building on the transition from 2G to 4G LTE. At each step of this evolution, operators and standards bodies learn from the past and adapt. IMSI encryption for network traffic is one example of a standard that has evolved for 5G. 3GPP's security working group approved the inclusion of Curve25519 for the Elliptic Curve Integrated Encryption Scheme ("ECIES"), which will improve network security.[27]

CTIA urges NIST to expand its discussion of network security and develop the network security standards in Appendix D. The NSTAC report to the President on Internet and Communications Resilience provides a helpful overview of the complexities and best practices used by network operators to mitigate threats such as botnets and distributed denial of service attacks.[28]

NIST also should broaden the discussion of connected vehicles, coordinating with subject matter experts in the Department of Transportation ("DOT") as appropriate. Section 7.2 (Connected Vehicles, IoT Cybersecurity Objectives, Risks, and Threats) largely omits recent developments by the auto sector to address cybersecurity. In addition to the various industry- and SDO-led standards and best practices, the DOT's National Highway Traffic Safety

---

[26] Nicole Cieslak, *NIST Cybersecurity Framework Adoption on the Rise*, Tenble (Mar. 29, 2016), https://www.tenable.com/blog/nist-cybersecurity-framework-adoption-on-the-rise.

[27] *See* Karl Norrman and Prajwol Kumar Nakarmi, *Protecting 5G Against IMSI Catchers*, Ericsson (June 29, 2017), https://www.ericsson.com/research-blog/protecting-5g-imsi-catchers/.

[28] *See* NSTAC, Report to the President on Internet and Communications Resilience (Nov. 16, 2017), https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20%2810-12-17%29%20%281%29-%20508%20compliant_0.pdf ("NSTAC Report to the President").

Administration ("NHTSA") has helped shepherd cybersecurity standards for connected vehicles. NHTSA has developed a core set of best practices to assist the auto industry in improving motor vehicle cybersecurity,[29] as well as released guidance on how to apply the NIST Cybersecurity Framework to modern vehicles.[30] The agency has also encouraged the automotive industry to form an Information Sharing Analysis Center ("ISAC") to quickly and uniformly respond to cybersecurity threats. Through this public-private partnership, participants voluntarily share cyber vulnerabilities and threat information to mitigate potential harms. NHTSA's partnership efforts, including its work with SAE International, are well documented.[31]

E. NIST should focus on the federal government and clarify its use cases.

Draft NISTIR 8200 notes that the "intended audience is both the government and public. The purpose is to inform and enable policymakers, managers, and standards participants as they seek timely development of and use of such standards in IoT components, systems, and services."[32] Shaping standards for the federal government is consistent with NIST's mission to help federal systems, which is reflected in numerous laws and NIST's description of its authority.[33] Government IT managers and other users of IoT devices face different expectations than private sector entities. If NIST tries to address federal and private users in a consolidated fashion, it risks blurring concepts and pushing solutions that may not match organizations' needs. NIST should clarify when standards are applicable for federal users and clearly emphasize the voluntary nature of such standards for private entities.

NIST also should more accurately identify the relevant stakeholders. In some use cases, the audience is incomplete or unclear.

- In Section 5.3 (Health IoT and Medical Devices, Examples of IoT Applications), NIST states that "wireless telecommunications companies have developed smart sensors that support wearable and implantable, injectable, and ingestible medical devices."[34] This is

---

[29] NHTSA, *Cybersecurity Best Practices for Modern Vehicles*, Report No. DOT HS 812 333 (Oct. 2016), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf; NHTSA, Automated Driving Systems 2.0: A Vision for Safety (Sept. 2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf.

[30] NHTSA, National Institute of Standards and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles, Report No. DOT HS 812 073 (Oct. 2014), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/812073_natlinstitstandardstechcyber.pdf.

[31] *See* NHTSA, NHTSA and Vehicle Cybersecurity (2016), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/nhtsavehiclecybersecurity2016.pdf.

[32] *See*, Draft NISTIR 8200, at iii.

[33] *See, e.g.*, Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq*., Public Law (P.L.) 113-283. S*ee also*, Draft NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations, at I (Aug. 2017) ("NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems[.]") ("Draft SP 800-53, Rev. 5").

[34] Draft NISTIR 8200, at 14.

not quite right; many organizations other than "telecommunications companies" have developed these devices and underlying components.

- In Section 7.3 (Consumer IoT, IoT Cybersecurity Objectives, Risks, and Threats), NIST should note the role that end users play in security.[35] Consumer inaction or choice can defeat what NIST might consider "adequate cybersecurity safeguards."[36]

- In Section 7.4 (Health IoT and Medical Devices, IoT Cybersecurity Objectives, Risks, and Threats), NIST identifies as a risk the "failure to provide timely security software updates."[37] However, the agency does not identify who is responsible for timely deployment, nor does it mention the risks from failure of enterprises, health care managers, or end users to deploy or accept updates. NIST should acknowledge these complexities where it discusses "threats."

NIST should remain focused on security. In a use case in Section 5.5 (Smart Manufacturing, Examples of IoT Applications"), NIST finds it problematic that "smart manufacturing environments are custom solutions that are complicated, expensive, and built on proprietary communications."[38] The only support NIST offers for its call to standardize "common security and communication standards" is to "lower the cost of entry" for small and medium businesses.[39] This sounds more like an economic than a security concern, but in any event, diversity in approaches can be desirable, particularly if it makes it more difficult for bad actors to exploit a single type of vulnerability. NIST should make clear that openness must be voluntary and note the tradeoffs of standardization.

IV. DEVELOPMENT OF DIVERSE THIRD-PARTY CERTIFICATION REGIMES WILL HELP IMPROVE SECURITY FOR AGENCIES AND THE PRIVATE SECTOR.

A. NIST is well positioned to promote diverse certification regimes.

Without picking winners and losers, agencies should utilize best practices and private certifications relevant to their IoT needs. The federal government should support private certification regimes that can be designed for varied settings and which, as stated in the Draft Report, can adjust to "society's need[s]."[40]

Industry-driven certification systems can enhance security, and NIST should promote their voluntary adoption worldwide. The Commission on Enhancing National Cybersecurity in its *Report on Securing and Growing the Digital Economy*, has recognized that continued U.S.

---

35 *Id.* at 41.

36 *Id.*

37 *Id.*, at 43.

38 *Id.*, at 20.

39 *Id.*

40 *See id.*, at 56.

leadership on cybersecurity requires international coordination.[41] The NSTAC *Report to the President on Internet and Communications Resilience* further underscored this point: "[NTIA and NIST] should work with device makers to facilitate the development of a baseline of recommended common sense security practices consistent with the risk associated with a device. [The Department of Commerce] should also review the role and viability of voluntary device certification and independent testing to ensure device security."[42]

DHS has stated that IoT security should be built on recognized security practices: "[s]tart with basic software security and cybersecurity practices and apply them to the IoT ecosystem in flexible, adaptive, and innovative ways."[43] Further, "risk-based security standards should be scalable and tailored to the direct impacts of a device or system being compromised[.]"[44] Because there is no one-size-fits-all approach, efforts must be flexible to accommodate different technologies and risk profiles. Certification by private groups and third parties can help ensure that devices meet desired security standards. Several groups are developing security programs. Underwriters Laboratories ("UL") offers a Cybersecurity Assurance Program ("CAP") to test and certify IoT devices, including devices developed for use within critical infrastructures or healthcare. The CAP uses standards developed as part of a voluntary program with technical experts from industry, the U.S. government, and academia.[45] Likewise, ISO is working on cybersecurity frameworks and IoT applications. International organizations affiliated with wireless stakeholders are particularly active:

- The Groupe Spéciale Mobile Association ("GSMA"), has issued IoT guidelines.[46] GSMA covered multiple topics, including solutions in the IoT ecosystem,[47] mitigating threats,[48] endpoint security,[49] and guidance for network operators.[50]

---

41 Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy,* 5 (Dec. 1, 2016), https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf ("As the global leader for innovation, the United States must be a standard-bearer for cybersecurity. This leadership requires investing in research and collaborating with other nations, including on international cybersecurity standards.") ("CENC Report").

42 NSTAC Report to the President, at 2.

43 DHS, Strategic Principles for Securing the Internet of Things (IoT), Version 1.0, at 9 (Nov. 15, 2016).

44 *See* CENC Report, at 24.

45 *See* UL, Cybersecurity: Securing and Protecting Products, Software, and Infrastructure against Cybersecurity Risks, https://industries.ul.com/cybersecurity.

46 *See* GSM Association, GSMA IoT Security Guidelines—Complete Document Set (Feb. 9, 2016), https://www.gsma.com/iot/gsma-iot-security-guidelines-complete-document-set/.

47 GSM Association, GSMA IoT Security Guidelines—Overview Document, Version 1.1 (Nov. 7 2016), https://www.gsma.com/iot/wp-content/uploads/2017/04/CLP.11-v1.1-Overview.pdf.

48 GSM Association, GSMA IoT Security Guidelines—Service Ecosystems, Version 1.1 (Nov. 7 2016), https://www.gsma.com/iot/wp-content/uploads/2017/04/CLP.12-v1.1-Service-Ecosystems.pdf.

49 GSM Association, GSMA IoT Security Guidelines—Endpoint Ecosystems, Version 1.1 (Nov. 7 2016), https://www.gsma.com/iot/wp-content/uploads/2017/04/CLP.13-v1.1-Endpoint.pdf.

50 GSM Association, GSMA IoT Security Guidelines—Network Operators, Version 1.1 (Sept. 2016), https://www.gsma.com/iot/wp-content/uploads/2017/04/CLP.14-v1.1-Network-Operators.pdf.

GSMA also established a voluntary IoT security assessment[51] and published guidance on IoT authentication using SIM cards.[52]

- The European Telecommunications Standards Institute ("ETSI") is developing voluntary standards for IoT security, including for smart appliances, smart cities, smart metering, eHealth, intelligent transport systems, and industrial automation.[53]

- IEEE offers a toolkit with information on a number of IoT issues, including IoT privacy and security.[54] Additionally, the IEEE Xplore digital library provides a wealth of technical information from cybersecurity experts.[55]

- A strategic initiative by global standards group oneM2M aims "to confront the critical need for a common M2M [Machine to Machine] Service Layer, . . . oneM2M will also develop globally agreed-upon M2M end-to-end specifications using common use cases and architecture principles across multiple M2M applications."[56]

- The Alliance for Telecommunications Industry Solutions ("ATIS") conducted a study on relationships and partnering between network operators and IoT service providers to illustrate ways to address IoT security concerns.[57]

- 3GPP Released 13 and 14 included specifications for secure IoT connectivity.[58]

NIST previously surveyed the cybersecurity work of SDOs.[59] It noted that "[c]ollectively, these SDOs have many hundreds of cybersecurity standards projects under maintenance or development. [And b]eing able to influence cybersecurity standards development requires developing and maintaining effective liaisons and active engagements

---

[51] GSM Association, IoT Security Assessment Process (2016), https://www.gsma.com/iot/iot-security-assessment/.

[52] GSM Association, Solutions to Enhance IoT authentication Using SIM Cards (UICC) (Nov. 2017), https://www.gsma.com/iot/wp-content/uploads/2017/05/cl_iot_authenticate_report_web_05_17.pdf.

[53] *See ETSI, Internet of Things—Our Role & Activities,* http://www.etsi.org/technologies-clusters/technologies/internet-of-things.

[54] *See* IEEE, Internet of Things Toolkit, http://iot.ieee.org/about/ieee-iot-toolkit.html.

[55] *See* IEEE, Xplore Digital Library, http://ieeexplore.ieee.org/Xplore/home.jsp.

[56] ATIS, About oneM2M, http://www.atis.org/oneM2M/about.asp.

[57] ATIS, Securing Internet of Things (IoT) Services Involving Network Operators (May 2017), https://access.atis.org/apps/group_public/download.php/34714/ATIS-I-0000056.pdf.

[58] Philippe Reininger, 3GPP Standards for the Internet of Things, 3GPP (Nov. 2016), ftp://www.3gpp.org/Information/presentations/presentations_2016/2016_11_3gpp_Standards_for_IoT.pdf; 3GPP, 3GPP Work Items associated with Specification (Aug. 1, 2017), http://www.3gpp.org/DynaReport/SpecVsWi--33860.htm.

[59] *See* NISTIR 8074, Volume 1, Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity (Dec. 2015).

within and among these SDOs."[60] Voluntary, industry-led certifications ensure that evaluation is informed by stakeholders, properly aligned with international standards, and flexible. NIST should make ample room for diverse efforts and champion voluntary certifications and standards.

B. Agencies should not utilize labeling as an approach to characterize security levels.

CTIA is pleased that Draft NISTIR 8200 encourages agencies to promote private conformity assessments,[61] but the agency should not emphasize consumer-facing logos or labeling.[62] Uniform labels are not likely to be applicable across sectors and may undermine the core principle of risk-based decision making. Without context, labels may convince users that a device is secure and discourage other security precautions.[63] Labels are likely to oversimplify IoT security. The Draft Report references the Wi-Fi™ logo. Although the Wi-Fi™ logo has become a useful and intuitive display for Internet connectivity, it reflects only one verifiable product characteristic: a device with that logo will connect to the user's WiFi network. As underscored in the Draft Report, cybersecurity in IoT is complex. Draft NISTIR 8200 identifies eleven major areas.[64] A simple logo is unlikely to convey accurate information to consumers about cryptography, incident management, IT system security evaluation, identity and access controls, network security, software assurances, or many other aspects of IoT security. As indicated by the five major examples of IoT "applications,"[65] there is a broad range of considerations across use cases.

V. NIST SHOULD STREAMLINE GOVERNMENT IOT EFFORTS AND ENGAGE MORE WITH STAKEHOLDERS ONGOAL SETTING.

NIST should be a leader in streamlining the many government efforts on IoT security and it should work closely with the private sector early in its agenda-setting to be sure its priorities match those of the community it aims to help.

Government agencies should harmonize their work and "focus on risk management—reducing industry's cost of complying with prescriptive or conflicting [initiatives] that may not aid cybersecurity and may unintentionally discourage rather than incentivize innovation."[66] In the Department of Commerce alone there are multiple lines of effort related to IoT security. NIST has ambitious IoT-related goals and a substantial role in Administration cybersecurity

---

60 *Id.*, at 7.

61 *See* Draft NISTIR 8200, at 56 ("US industry has a rich history of developing conformity assessment (CA) programs to meet our society's needs.").

62 *See id.*, at 56.

63 *See* U.S. Chamber of Commerce, *The IoT Revolution and Our Digital Security*, 26 (Sep. 2017), https://www.uschamber.com/IoT-security.

64 *See id.*, at 22-31.

65 *See id.*, at 9.

66 CENC Report, at 20.

efforts.[67] Along with Draft NISTIR 8200, various workflows are taking place at NIST, with more than twenty listed under *NIST Initiatives on IoT*.[68] Some examples:

- NIST's Cybersecurity for IoT Working Group[69] has initiated a series of roundtables, stakeholder meetings, and colloquia[70] with the goal of producing a document on IoT security and privacy risks.[71]

- Draft Special Publication ("SP") 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, was introduced last summer.[72] It is "a comprehensive set of security and privacy safeguarding measures for all types of computing platforms, including…the Internet of Things (IoT)."[73]

- The National Cybersecurity Center of Excellence ("NCCoE") is looking at IoT, launching projects on *Mitigating IoT-Based DDoS*[74] and *Identity and Access Management for Smart Home Devices,*[75] among others.

In 2016 and 2017, the National Telecommunications and Information Administration ("NTIA") convened a multistakeholder process on IoT security patching and upgradability.[76] More work may commence. Varied agencies, from DHS to the Federal Trade Commission and the Consumer Products Safety Commission are looking at IoT as well.[77]

NIST should coordinate internally and with other agencies to reduce overlap. As a recent report to the President explained, "[t]he government should consolidate and coordinate efforts to strengthen the Nation's cybersecurity more efficiently. For example, there have been several

---

67 *See* Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, EO 13800 (May 11, 2017).

68 *See* NIST Initiatives in IoT, https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot.

69 *See* NIST Cybersecurity for IoT Program, https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program.

70 *See* NIST, IoT Cybersecurity Colloquium (Oct. 19, 2017), https://www.nist.gov/news-events/events/2017/10/iot-cybersecurity-colloquium.

71 *See* NIST, *IoT Security and Privacy Risk Considerations* (Dec. 20, 2017), https://www.nist.gov/sites/default/files/documents/2017/12/20/nist_iot_security_and_privacy_risk_considerations_discussion_draft.pdf.

72 *See* Draft SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations (Aug. 2017) ("Draft SP 800-53, Rev. 5").

73 *Id.*, at v.

74 *See* NCCoE, Mitigating IoT-Based DDoS, https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos.

75 *See* NCCoE, Identity and Access Management for Smart Home Devices, https://www.nccoe.nist.gov/projects/project-concepts/idam-smart-home-devices.

76 *See* NTIA, Multistakeholder Process: Internet of Things (IoT) Security Upgradability and Patching, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

77 *See*, e.g., CPSC, *The Internet of Things and Consumer Product Hazards,* Notice of Public Hearing and Request for Written Comments, 83 Fed. Reg. 13122 (Mar. 27, 2018).

overlapping efforts to improve supply chain security from a variety of agencies including NIST, DHS, and the FCC. There have also been overlapping efforts for IoT security, including at DHS, NIST, and NTIA, as well as at multiple agencies who oversee the various IoT verticals (such as vehicles, Smart Cities etc.)."[78]

Likewise, NIST should ensure that its agenda is coordinated with the private sector experts that it hopes will use its documents. As NIST has stated, a "multi-stakeholder approach leverages the respective strengths of the public and private sectors, and helps develop solutions in which both sides will be invested."[79] A private-sector led approach is fundamental because it "does not dictate solutions to industry, but rather facilitates industry coming together to offer and develop solutions that the private sector is best positioned to embrace."[80]

Finally, private stakeholder input is critical as NIST sets its agenda, which increasingly looks at the private sector and privacy. This was evident in Draft Special Publication 800-53 revision 5 ("[f]ully integrating the privacy controls into the security control catalog")[81] and is apparent in ongoing workshops about IoT. As NIST states in its Cybersecurity for IoT Program, it is looking at "privacy issues with IoT devices" and observes that "[i]nformed consent involves becoming fully aware of consequences. The IoT landscape is making this increasing[ly] difficult and making consent revocation and data deletion increasingly harder to attain."[82] NIST should proceed with caution and fully engage the private sector on fundamental questions, not just details. Inadequate consultation can yield efforts that are not adopted and do not promote security. Engaging industry to develop priorities would be the most efficient use of government and private resources, reducing the likelihood of duplicative efforts.

VI. CONCLUSION

CTIA is encouraged by NIST's continued support for cybersecurity standards developed by international, industry-led standards bodies. These organizations have the reach to enhance and facilitate IoT security, while promoting open markets with free and open cross-border data flows, economies of scale, and interoperability. CTIA proposes several changes to Draft NISTIR 8200. NIST should confirm the voluntary nature of the standards identified, and more fully acknowledge ongoing activity to address security. NIST should also not attempt to characterize implementation or adequacy of standards that exist. This is particularly salient in the discussion of network security and Table 4.

Rather than labeling, NIST should encourage agencies to foster private innovation and development of appropriate certifications. CTIA encourages NIST to engage industry

---

78 NSTAC Report to the President, at 35-36.

79 Testimony of Dr. Patrick Gallagher, Director, NIST, before the United States Senate Committee on Commerce, Science, and Transportation (July 25, 2013), https://www.nist.gov/speech-testimony/partnership-between-nist-and-private-sector-improving-cybersecurity.

80 *Id.*

81 Draft NIST SP 800-53, Rev. 5, at v.

82 NIST, NIST Cybersecurity for IoT Program Overview, https://csrc.nist.gov/CSRC/media/Presentations/NIST-Cybersecurity-for-IoT-Program/images-media/NIST%20Cybersecurity%20for%20IoT%20Program.pdf.

stakeholders by leveraging private sector expertise prior to launching cyber and IoT initiatives. Importantly, the agency should promote better coordination and support streamlining efforts within the U.S. government. These efforts to promote more efficient, effective, and coordinated uses of resources will serve as an example to other countries and help secure our digital future.

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

April 18, 2018