Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

In the Matter of	)	
	)	
Cybersecurity in the Digital Ecosystem	)	Docket No. 150312253-5253-01
	)	
	)	

Comments of
CTIA – The Wireless Association®, the
Alliance of Automobile Manufacturers, the
Association of Global Automakers, and the
Intelligent Car Coalition

Robert Strassburger
Vice President, Vehicle Safety and Harmonization

Will Otero
Director, Transportation and Safety Policy

ALLIANCE OF AUTOMOBILE MANUFACTURERS
803 7th Street, NW, Suite 300
Washington, DC 20001
(202) 326-5500

Thomas Sawanobori
Senior Vice President, Chief Technology Officer

John Marinho
Vice President, Technology and Cybersecurity

CTIA – THE WIRELESS ASSOCIATION®
1400 16th Street, NW, Suite 600
Washington, DC 20036
(202) 785-0081

Michael X. Cammisa
Senior Director, Safety

ASSOCIATION OF GLOBAL AUTOMAKERS, INC.
1050 K Street, NW, Suite 650
Washington, DC 20001
(202) 650-5554

Catherine McCullough
Executive Director

INTELLIGENT CAR COALITION
1155 F Street, NW, Suite 1050
Washington, DC 20004
(202) 559-8780

TABLE OF CONTENTS

Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

In the Matter of	)	
	)	
Cybersecurity in the Digital Ecosystem	)	Docket No. 150312253-5253-01
	)	
	)	

Comments of
CTIA – The Wireless Association®, the
Alliance of Automobile Manufacturers, the
Association of Global Automakers, and the
Intelligent Car Coalition

CTIA – The Wireless Association® ("CTIA"),[1] the Alliance of Automobile Manufacturers,[2] the Association of Global Automakers,[3] and the Intelligent Car Coalition[4] (collectively, the "Automotive Associations") welcome the opportunity to provide the following

[1] CTIA – The Wireless Association® is the international organization of the wireless communications industry for both wireless carriers and manufacturers. Membership in the organization covers Commercial Mobile Radio Service ("CMRS") providers and manufacturers, including cellular, Advanced Wireless Service, 700 MHz, broadband PCS, and ESMR, as well as providers and manufacturers of wireless data services and products.

[2] The Alliance of Automobile Manufacturers is an association of 12 vehicle manufacturers, including BMW Group, FCA US LLC, Ford Motor Company, General Motors Company, Jaguar Land Rover, Mazda, Mercedes-Benz USA, Mitsubishi Motors, Porsche, Toyota, Volkswagen Group of America, and Volvo Cars North America. It is the leading advocacy group for the auto industry, representing over 70% of all car and light truck sales in the United States.

[3] The Association of Global Automakers represents international motor vehicle manufacturers, original equipment suppliers, and other automotive-related trade associations. Its members include American Honda Motor Co., Aston Martin Lagonda of North America, Inc., Ferrari North America, Inc., Hyundai Motor America, Isuzu Motors America, Inc., Kia Motors America, Inc., Maserati North America, Inc., McLaren Automotive Ltd., Nissan North America, Inc., Subaru of America, Inc., Suzuki Motor of America, Inc., and Toyota Motor North America, Inc.

[4] The Intelligent Car Coalition is a group of telecommunications, automaker, and auto supplier stakeholders that articulates the benefits of connected car technologies and advocates for public policies that bring the innovations at the intersection of automotive and communications technologies to consumers. It is the only group in Washington, D.C. devoted exclusively to resolving policy on connected car issues.

comments in response to the Department of Commerce's Internet Policy Task Force ("IPTF") Request for Public Comment ("RFC") regarding cybersecurity issues facing the digital economy.[5]

I. INTRODUCTION

CTIA represents all contributors to the global wireless ecosystem, from manufacturers and carriers to software and application developers. Through collaboration and innovation, these contributors have led a mobile revolution that has transformed the global economy.

Wireless service providers and automakers operate in a cybersecurity threat environment that is dynamic and asymmetric. CTIA has worked for years with its members and policy makers to develop adaptive solutions to these security and technology challenges. As a result, the wireless industry has led the way on cybersecurity and is actively engaged through public-private partnerships in the U.S. and through international standards-setting bodies.

Automakers use various strategies to design and build safe and secure vehicles. These strategies include robust process standards for product development, extensive testing and validation, diagnostics, provision of fail-safe mechanisms, controlled network gateways, and controlled fleet tests on public roadways. Proprietary standards and practices are also used by individual vehicle manufacturers and were developed internally over many years. In many cases, automakers and suppliers converge over time on similar "best practices" to ensure robust system functionality in the field, and standards are then formalized by standards developing organizations ("SDOs"), including the Society of Automotive Engineers ("SAE"), the Institute of

[5] *See* Department of Commerce, *Stakeholder Engagement on Cybersecurity in the Digital Ecosystem*, 80 Fed. Reg. 14360 (Mar. 19, 2015) ("RFC"), *available at* http://www.ntia.doc.gov/files/ntia/publications/cybersecurity_rfc_03192015.pdf.

Electrical and Electronics Engineers ("IEEE"), and the International Organization for Standardization ("ISO").

In addition, automakers are collaborating on two initiatives to further enhance auto industry practices and standards. First, automakers have developed consumer privacy protection principles.[6] Development of the principles reflects a major unified step in protecting personal information collected by vehicles. For the first time, the industry is working to adopt central principles to demonstrate a unified commitment to the responsible stewardship of information used to provide vehicle technologies and services. The establishment of these principles complements a second collective action by automakers to help ensure the security of vehicle-generated data. In July 2014, automakers began collaborating on the creation of a voluntary center to share and analyze potential cyber-related threats and vulnerabilities in the automotive sector.[7] This effort represents yet another significant step forward in protecting data privacy and data security in the automotive industry

Cybersecurity threats are not limited to the wireless or automotive sectors, however. They affect the entire Internet ecosystem. No one actor or industry segment can act alone to prevent, detect, or mitigate these threats; all parts of the ecosystem must work together. IPTF's efforts in this regard are critical. CTIA and the Automotive Associations therefore strongly support IPTF's efforts and believe that the Department of Commerce is uniquely suited to convene representatives from industry sectors that have a significant role to play in

[6] Auto Alliance, "Privacy Principles for Vehicle Technologies and Services," http://www.autoalliance.org/?objectid=865F3AC0-68FD-11E4-866D000C296BA163.

[7] *See, e.g.*, Letter from the Alliance of Automobile Manufacturers, Inc. and the Association of Global Automakers to the National Highway Traffic Safety Administration, Docket No. NHTSA-2014-0071 (Oct. 16, 2014).

cybersecurity, but that are not critical infrastructure companies that participated in the development of the NIST cybersecurity framework ("NIST Framework").

CTIA and the Automotive Associations recommend that IPTF use the same industry-led process that NIST used to facilitate the development of the NIST Framework as a model for an industry-led process to develop a comparable high-level, voluntary cybersecurity framework for the rest of the online ecosystem. The NIST Framework provides a useful template because it gives industry the flexibility to improve security and user trust while allowing innovation—consistent with the RFC's goal of focusing on security challenges "where collaborative voluntary action between diverse actors can substantially improve security for everyone."[8]

The communications industry participated in the development of the NIST Framework and in recent efforts to align cybersecurity guidelines and practices for the telecommunications sector with the NIST Framework. Those efforts were led by the Communications Security, Reliability and Interoperability Council ("CSRIC") IV, which is a voluntary, cooperative, *industry-led effort* with the FCC in the role of convener. CTIA and the Automotive Associations expect this industry-led, government-supported approach to allow them to strengthen their cybersecurity programs without impeding their business objectives or ability to innovate.

As described in the RFC, IPTF seeks comment on which cybersecurity-related topics could be best addressed by a consensus-based multistakeholder process to develop voluntary guidelines and practices for industry. As explained in detail below, CTIA and the Automotive Associations recommend that the process address both short-term and long-term issues, but it should first identify and focus on several short-term issues that can be resolved relatively easily.

[8] RFC at 5.

By achieving early success on those issues, the multistakeholder effort will generate positive momentum and will lay a strong foundation from which to resolve the more complex challenges.

II. A MULTISTAKEHOLDER APPROACH THAT ENGAGES ALL RELEVANT INDUSTRY SECTORS IS ESSENTIAL

A. The Multistakeholder Process Should Involve All Relevant Industry Sectors Throughout the Interconnected Online Ecosystem.

Any entity that has an online presence faces cybersecurity risks and is a potential victim of, and conduit for, cybersecurity threats. These threats, in turn, may pose risks to other entities connected to the network. All parts of the ecosystem, including software developers, search providers, retail and e-commerce sites, healthcare providers, and others, must work collectively to develop effective security solutions. Therefore, identifying and convening the essential participants at the outset should be IPTF's first objective.

Thus far, other cybersecurity initiatives have focused on a subset of industry sectors. For example, Executive Order 13636 focused on improving industry sectors that constitute "critical infrastructure."[9] Similarly, the FCC's CSRIC works on cybersecurity issues that affect the communications sector.[10] Those efforts have developed useful cybersecurity frameworks and guidelines for those industries. These efforts, however, did not include other important industry sectors, such as healthcare, finance, and retail, all of which have experienced serious cybersecurity incidents.

Several of the biggest and most recent harmful incidents occurred at companies that were not part of critical infrastructure. For instance, a health insurer, Anthem, Inc., announced earlier this year that it had suffered a data breach that affected nearly 80 million insureds, exposing their

[9] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2013), http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[10] *See* Description of CSRIC, http://transition.fcc.gov/pshs/advisory/csric/.

names, birthdates, and Social Security Numbers.[11] Similarly, the data breach at Sony Pictures Entertainment in December 2014 exposed reams of sensitive data, including employees' health information, Social Security Numbers, dates of birth, and federal tax records, as well as proprietary company information.[12] Indeed, according to Verizon's 2015 Data Breach Investigations Report ("DBIR"), several industry sectors that experienced the largest numbers of security incidents and confirmed data losses last year were manufacturing, retail, professional services, and accommodations, none of which was addressed during the multistakeholder process to develop the NIST Framework.[13]

This new multistakeholder process gives IPTF an opportunity to close gaps in cybersecurity preparedness by engaging these other commercial sectors. The multistakeholder process can provide these sectors with an overarching framework and a common lexicon that will allow them to develop business-specific cybersecurity programs and communicate across industry sectors. This process will do more than bring previously unaddressed industry sectors into the fold, however. As the DBIR noted, "many subsectors in different industries actually share a closer threat profile than do subsectors in the same overall industry."[14] Therefore, not only will addressing the cybersecurity of non-critical infrastructure industry sectors improve cybersecurity protection across the network, it may also reveal unknown risks for critical

[11] *See* Charles Ornstein, *Health Data Breaches Sow Confusion, Frustration*, USA Today, Apr. 14, 2015, http://www.usatoday.com/story/money/2015/04/14/hacking-health-data-privacy/25597337/.

[12] *See Sony Breach May Have Exposed Employee Healthcare, Salary Data*, KrebsOnSecurity, Dec. 14, 2014, http://krebsonsecurity.com/2014/12/sony-breach-may-have-exposed-employee-healthcare-salary-data/.

[13] Verizon, 2015 Data Breach Investigations Report, at 3, http://www.verizonenterprise.com/DBIR/2015/.

[14] *Id*. at 25.

infrastructure sectors, allowing critical infrastructure sectors to continue modifying and adapting their risk profiles.

B. The Department of Commerce is Uniquely Suited to Convene These Various Stakeholders.

Unlike other regulatory bodies that may have a role to play in developing cybersecurity guidelines for the specific sectors that they regulate, the Department of Commerce is uniquely suited to convene participants from a wide range of industries.[15] Indeed, the Department of Commerce has a history of successfully convening representatives from various industry sectors to find common ground on these issues.[16]

NTIA's association with the Internet Corporation for Assigned Names and Numbers ("ICANN") is particularly important. NTIA's experience with ICANN on issues such as Domain Name System ("DNS") security gives NTIA the credibility to address security issues,[17] and NTIA's history with ICANN gives it the ability to reach other entities in the IT sector that did not participate in the development of the NIST Framework.

---

[15] For instance, as discussed earlier, the FCC has played an active role in working with industry through the CSRIC to transpose the NIST Framework into industry best practices for each subsector of the communications industry. Similarly, the National Highway Traffic Safety Administration ("NHTSA") has worked with the automotive industry to develop cybersecurity best practices and guidelines. *See* NHTSA Automotive Cybersecurity Topics and Publications, http://www.regulations.gov/#!docketDetail;D=NHTSA-2014-0071.

[16] The Department of Commerce's recent work through NIST with critical infrastructure industry representatives to develop the NIST Framework is an excellent example. Similarly, NTIA's participation in the multistakeholder processes to develop a voluntary code of conduct for the commercial use of facial recognition technology, and a voluntary code that enhances transparency in how companies that provide applications and interactive services for mobile devices handle personal data, demonstrate its success in this convener role.

[17] *See, e.g.*, Department of Commerce, National Telecommunications and Information Administration, *Enhancing the Security and Stability of the Internet's Domain Name and Addressing System*, 73 Fed. Reg. 197 (Oct. 9, 2008), http://www.ntia.doc.gov/files/ntia/publications/fr_dnssec_081009.pdf.

Finally, unlike some other regulatory bodies, NTIA can consider global factors, which are critical given the borderless nature of cybersecurity threats.[18] Indeed, as the Government Accountability Office has noted, NTIA is "responsible for activities that can impact international efforts related to cyberspace security and governance."[19] As IPTF engages stakeholders, it should take into account the efforts of a number of national and global standard-setting groups that have played an important role in the global mobile ecosystem. IPTF can leverage the work that these groups have done in facilitating the development of a framework.

III. THE NIST CYBERSECURITY FRAMEWORK SHOULD SERVE AS THE BASIS FOR THE MULTISTAKEHOLDER PROCESS

Participants in the process to develop the NIST Framework—including the wireless industry—widely view that process as a successful example of a productive multistakeholder effort, in large part because industry led the effort. IPTF should take the same industry-led approach here. In particular, IPTF should use the same industry-led process that NIST used to facilitate the development of the NIST Framework as a model to facilitate the development of a comparable voluntary, risk-based and outcome-based approach to cybersecurity, rather than a prescriptive checklist of activities. Doing so would be consistent with the RFC's recognition that traditional regulation in this context is "difficult and inefficient" in light of the "pace of innovation in the highly dynamic digital ecosystem."[20]

A voluntary, flexible framework will enable entities to modify their approach to respond to threats as they evolve. Such a framework can scale, allowing entities to adapt their particular

---

[18] *See* White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (May 29, 2009) (discussing the importance of global cooperation and involvement to develop technical standards and norms).

[19] Government Accountability Office, *United States Faces Challenges in Addressing Global Cybersecurity and Governance*, GAO-10-606 (July 2010) at 18, http://gao.gov/assets/310/308401.pdf.

[20] RFC at 3.

cybersecurity efforts to fit their unique business models, infrastructure, and the assets they need to protect. The RFC rightly observes that such voluntary, coordinated action is preferable to prescriptive regulation, stating that "[i]n the digital ecosystem, the rapid pace of innovation often outstrips the ability of regulators to effectively administer key policy questions," and that "[o]pen, voluntary, and consensus-driven processes can work to safeguard the interests of all stakeholders while still allowing the digital economy to thrive."

CTIA members can attest to the value of this approach. As mentioned above, the communications sector used the NIST Framework in CSRIC IV, its most recent collaborative effort, to develop specific cybersecurity guidelines for five segments of the telecommunications industry: wireless, wireline, broadcast, cable, and satellite.[21] Each industry segment had different cybersecurity needs and methods for achieving their goals. The NIST Framework gave the industry enough flexibility to develop security programs that scale to meet each industry segment's unique needs. Likewise, use of a similar framework here that also is voluntary, risk- and outcome-based, and flexible will produce the sort of "fair, voluntary, and stakeholder-driven" outcomes that the RFC envisions.

IV. IPTF SHOULD PRIORITIZE ISSUES THAT CAN READILY BE RESOLVED IN THE SHORT TERM

The RFC states that IPTF envisions a multistakeholder process that will address "discrete security challenges."[22] It then proceeds to identify some of those issues, while seeking comment on any that should be added to the list and, perhaps more to the point, on which challenges would be most amenable to resolution through the use of the proposed framework.[23] The RFC's

[21] *See* CSRIC, *Cybersecurity Risk Management and Best Practices Working Group 4: Final Report* (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[22] RFC at 5.

[23] *See generally id.* at 6-11.

lengthy recitation of possible issues and issue areas underscores that there is no shortage of cybersecurity issues that stakeholders must address—a list that is only likely to grow as further input is collected through this inquiry. Tackling all of them at once would not be practical or even advisable. Accordingly, some degree of prioritization is essential to ensure a manageable process and likely progress.

Fundamentally, CTIA and the Automotive Associations urge IPTF to conceptualize these various cybersecurity challenges in terms of what can be readily achieved in the short-term and what will require a longer timeframe. The objective is not to defer engaging in the more difficult and complex questions, but rather, to secure some early successes that will generate positive momentum to sustain the multistakeholder process as it progresses. This will lay the foundation for resolving the more complex challenges that will remain, such as global coordination and engagement, web security and consumer trust, and enabling markets and innovation. Indeed, these issues have deep roots and likely will require a multifaceted, time-intensive approach. To mention just one example, CTIA's in-house research reveals a gap between consumers' high awareness of the vulnerability of their mobile devices and the limited actions they generally take to protect themselves and their information.[24] Closing this gap between awareness and action will not occur overnight, but will instead require a persistent, long-term effort.

In the meantime, CTIA and the Automotive Associations suggest that IPTF focus initially on the following six areas. While this list is not necessarily exhaustive, it should illustrate the

[24] *See* CTIA, "Wireless Consumers are Aware of Cyberthreats and Know They Should Protect Themselves, Yet Many Don't," May 22, 2013 (press release) (summarizing Harris Interactive survey commissioned by CTIA), http://www.ctia.org/resource-library/press-releases/archive/wireless-consumers-cyberthreats-protect-themselves; *see also* Mary Madden & Lee Rainie, "Americans' Attitudes About Privacy, Security, and Surveillance," *Pew Research Center: Internet, Science & Tech*, May 20, 2015, http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ (describing similar survey results from the Pew Research Center).

extent to which the multistakeholder process could claim some quick victories that will instill confidence in the process going forward.[25] After such short-term objectives are met, the stakeholders can turn their attention to the long-term issues.

1. Distributed denial of service ("DDoS") attacks

Some industry participants—such as Symantec, Kaspersky Labs, and Trend Micro, among others—have done, or have reported on, extensive research regarding distributed denial of service ("DDoS") attacks. While these entities encourage companies to engage in advance preparation and develop anti-DDoS strategies, they also have recognized that DDoS attacks are difficult to stop entirely. Therefore, they have developed a good understanding of the most effective means of mitigating these attacks. Symantec, for instance, observes that while the use of techniques to address the risk of spoofing IP addresses will not completely eliminate DDoS attacks (since compromised servers and botnets could flood victims by using their real IP addresses), those techniques would make it harder for attackers to hide and would reduce the chances of amplification attacks.[26] In addition, Kaspersky Labs has devised solutions that require a connection channel between its cleaning centers (located on the Internet backbone) and a company's IT infrastructure, and it also has developed guidance regarding the choice of redirection methods to those channels (*i.e.*, Border Gateway Protocol (BGP) and DNS).[27] Others have noted the potential utility of combining a cloud-based anti-DDoS solution (which, by its

[25] In other words, this list is not intended to exclude from consideration other objectives, such as the need to address weak passwords, that may also be within reach in the near term.

[26] *See* Candid Wueest, Symantec, "The continued rise of DDoS attacks," Oct. 21, 2014, at 22-23, *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-continued-rise-of-ddos-attacks.pdf.

[27] *See* Kaspersky Labs, "Protecting your business against financial and reputational losses with Kaspersky DDoS Protection," at 5, *available at* http://media.kaspersky.com/pdf/Kaspersky_Lab_Whitepaper_Kaspersky_DDoS_Protection_final.pdf.

nature, is a non-demand solution, such that human intervention is needed to make the decision to enable a cut-over to the anti-DDoS cloud provider) with an always-on, on-premises DDoS defense.[28]

However, as CTIA has discussed previously,[29] and as the work of the security industry participants discussed above shows, some techniques for mitigating these attacks require collaboration with other players in the ecosystem, such as hosting providers. Indeed, DDoS attacks may largely originate from web hosting providers and large data centers. If hosting providers participated in the multistakeholder process, they could ensure that other stakeholders that tend to be reactive become proactive instead.

Thus, IPTF should reach out to hosting providers to enlist their participation in these efforts. While DDoS attacks are not necessarily the most critical cybersecurity threats, effective solutions are known and could readily be implemented. This would give the multistakeholder process an opportunity to show quick and substantial progress.

2. DNS amplification attacks

Relatedly, IPTF should work proactively with hosting providers to address DNS amplification attacks, a popular form of DDoS attack that uses publicly accessible DNS servers to flood a target system with DNS response traffic. Industry has developed some means of detecting and addressing the effects of DNS amplification attacks—allowing entities, if nothing else, to reduce the number of servers that attackers can use to generate the large volumes of

[28] Stephen Gates, "Overcoming the DDoS Challenge in 2015," *CIO Review*, http://symantec.cioreview.com/cxoinsight/overcoming-the-ddos-challenge-in-2015-nid-4884-cid-74.html.

[29] Comments of CTIA – The Wireless Association®, Cybersecurity Working Group, DA 14-1066, FCC, at 24 (filed Sept. 26, 2014).

traffic that these attacks require.[30] Engaging hosting providers in the near term to develop further methods of preventing and mitigating DNS amplification attacks would help other stakeholders, in all industry segments, to address this problem.

3. Information sharing and analysis organization ("ISAO") use cases

The sharing of threat intelligence indicators—not just between private sector entities and the government, but within the private sector itself—is a critical aspect of cybersecurity. Its importance cannot be overstated. Responding to the evolving threat environment requires companies to have access to the latest intelligence gathered by U.S. cybersecurity experts and the most innovative solutions.[31]

The process of cyber information sharing is becoming more complex. As CTIA has described at length, there are a number of obstacles to effective information sharing, ranging from antitrust concerns to privacy restrictions, among others.[32] Meanwhile, the volume of threat information that is being shared (and that could be shared) is increasing and could become unmanageable. Information sharing therefore must become automated to allow for real-time mitigation, while protecting privacy (for example, through the removal of personally identifiable information) and maintaining other necessary safeguards. Some more sophisticated threats may require systems to elevate certain information-sharing decisions in some circumstances to allow human involvement. For these reasons, among others, CTIA has urged Congress to adopt

---

[30] *See, e.g.*, US-CERT, Alert (TA13-088A): DNS Amplification Attacks, May 29, 2013, https://www.us-cert.gov/ncas/alerts/TA13-088A.

[31] *See* CTIA, *Today's Mobile Cybersecurity: Information Sharing*, Sept. 9, 2014, at 3 ("CTIA Information Sharing White Paper"), *available at* http://www.ctia.org/docs/default-source/default-document-library/ctia_informationsharing.pdf.

[32] *See, e.g.*, Comments of CTIA – The Wireless Association®, Guide to Cyber Threat Information Sharing (Draft), NIST Special Publication 800-150 (Draft), at 3-5 (filed Nov. 28, 2014) ("CTIA NIST Information Sharing Comments"); CTIA Information Sharing White Paper at 5.

cybersecurity information sharing legislation to provide legal certainty and enable real-time, information sharing capabilities.[33] For instance, the Cyber Intelligence Sharing and Protection Act ("CISPA") and Protecting Cyber Networks Act ("PCNA"), both of which remain pending, would alleviate many of the current impediments to information sharing and improve communication between players in the Internet ecosystem and the federal government.[34]

Notwithstanding these various challenges, carriers have developed effective mechanisms for information sharing in a trusted setting. As CTIA has described previously, CTIA's members have cultivated a variety of information-sharing organizations and relationships, facilitating both formal and informal information-sharing activities among a number of entities within the ecosystem.[35] However, other industry sectors—especially those, such as the retail sector, that have faced a disproportionate number of cyber threats—may not have had the same opportunities to share information, leaving them without analogous processes or comparable experience regarding the most effective ways to exchange threat information.

Closing such knowledge gaps is critical. Developing a small number of use cases based on the anticipated DHS standard for real-time automated information sharing will equip a range of entities across industry sectors with access to information sharing tools and strategies. Stakeholders can develop these use cases without first addressing the other obstacles to information sharing noted above. These use cases may provide entities with a trusted environment within which to share information, while stakeholders continue to address and attempt to resolve the policy and legal issues that can inhibit information sharing.

---

[33] *See, e.g.*, CTIA Information Sharing White Paper at 16.

[34] *See, e.g., id.*

[35] *See, e.g.*, CTIA NIST Information Sharing Comments at 5-6 (describing current information-sharing activities); CTIA Information Sharing White Paper at 9 (describing advances in information sharing during the last decade).

4. Training protocols for small and medium-sized organizations

As discussed above, all sectors of the economy must work together to address cybersecurity. This will require collaboration among all of the diverse entities that comprise the ecosystem. As NIST has recognized (and as CTIA and other trade groups have explained as well), these include organizations of different sizes with varying amounts of resources and internal expertise relevant to cybersecurity issues.[36] The NIST Framework thus properly does not seek to impose a one-size-fits-all solution. Instead, it offers a framework that can be scaled to a particular company's needs.

To further account for and address differences in how organizations of different sizes manage cybersecurity issues, IPTF should prioritize training that is oriented toward smaller and medium-sized organizations that may require additional guidance. Unlike large organizations, small and medium-sized organizations generally lack the resources to understand and address cybersecurity concerns as fully as is necessary in this complex and challenging environment. Thus, IPTF should focus in the near-term on curing the relative disadvantage that smaller and medium-sized organizations have in this area to ensure that all organizations are on equal footing. Closing that gap likely will require a multi-pronged approach, but a good first step would be to leverage the experience accumulated to date to develop and implement training protocols that highlight key issues and concerns. Such mechanisms and protocols could be made available online and/or through a series of regional workshops,[37] depending on the nature of the

[36] *See, e.g.*, Comments of CTIA – The Wireless Association®, the National Cable & Telecommunications Association, and US Telecom, Docket No. 130909789-3789-01, at 10 (filed Dec. 13, 2013).

[37] RFC at 12 (asking whether certain cybersecurity issues would be better served by a single workshop or event rather than a longer process).

training mechanism and on what method of access to this information proves to be most convenient for those that most need it.

5. Attack vectors

Cybersecurity responses tend to be reactive. Yet there is a growing awareness that future success in this area depends on a collective shift toward a more proactive approach. As NIST itself has recognized, "An organization should move from informal, ad hoc, reactive cybersecurity approaches where the organization operates in isolation to formal, repeatable, adaptive, proactive, risk-informed practices where the organization coordinates and collaborates with partners; such an approach is described in the Cybersecurity Framework."[38]

In order to become more proactive, entities will have to understand *in advance* what their points of vulnerability are and what types of threats they face. By better understanding threat trends and their evolution, entities will be able to anticipate and get ahead of problems before they suffer an attack. Today, for example, data breaches that commonly occur on point-of-sale ("POS") machines are a common and well-publicized problem, spurring industry to develop ways to determine the causes of those breaches and prevent them from occurring (or recurring). But after such machines are secure, cyber threats will migrate elsewhere, and new security solutions will be necessary. An optimal approach to cybersecurity will ensure that industry detects those future threats before they cause harm, rather than after damage has occurred.

The ability to anticipate problems is particularly important in connection with advanced persistent threats ("APTs"), which gain access to a network by combining different attack tools and vectors such as spear-phishing (whereby a malicious email or link is sent to specific individuals within an organization) and SQL injection (whereby an SQL query is inserted in an

[38] NIST, *Guide to Cyber Threat Information Sharing (Draft)*, Oct. 2014, at 19.

application to, among other things, read sensitive data). State actors often are responsible for these kinds of attacks. Such entities often have access to substantial resources, which in conjunction with certain factors—such as the degree of sophistication of the attack and the nature of the target, among other considerations—may heighten the need for assistance from the U.S. government.

IPTF thus should focus on developing processes that will facilitate education about threat trends and their evolution. It should consider establishing a trusted environment in which information about these threats can be shared without risk of liability or disclosure. These education sessions could take place sector-by-sector or within certain communities of interest to ensure joint participation by industries that are often integrated, such as the financial and telecommunications sectors. They could also involve a combination of informal and formal sessions, including workshops, as the RFC suggests, provided that the high-level conclusions ultimately are elevated to the broader multistakeholder level.[39]

6. Internet of Things

The Internet of Things ("IoT") is growing at a staggering rate and will involve ubiquitous connectivity, automated data sharing, and interoperability between and among a large number of vertical sectors, a range of platforms, device formats, and services. The IoT holds tremendous promise and potential to improve economic productivity, individual well-being, and energy efficiency. For instance, through wireless technology, connected cars will communicate with each another and with transportation infrastructure to improve safety, conserve energy, and ease

[39] *See, e.g.*, RFC at 12.

congestion.[40] While IoT devices are not immune from cybersecurity threats, top-down regulation would stifle growth and the proper functioning of machines and devices in the dynamic, always-on IoT environment.[41]

Other entities have recognized the need for flexibility in this area and already have begun to suggest best practices and to develop cybersecurity standards and solutions to ensure cybersecurity protection and interoperability in the IoT.[42] IPTF should review the work of these entities, including the Federal Trade Commission, the National Security Telecommunications Advisory Committee, private standards organizations, and others. IPTF's multistakeholder process would be a good venue through which to provide stakeholders with access to these materials so that they can adopt and implement them, as appropriate.

V. CONCLUSION

Every entity that is part of the Internet ecosystem is both vulnerable to and a potential conduit for cybersecurity threats. Therefore, all parts of the ecosystem must work collaboratively to develop solutions to prevent, detect, and mitigate these threats. NTIA is in a unique position to convene participants from all relevant industry sectors to do just that. CTIA and the Automotive Associations therefore strongly support NTIA's efforts, through IPTF, to convene a multistakeholder process to address cybersecurity threats to non-critical infrastructure industries. CTIA and the Automotive Associations encourage NTIA to use the process through which the NIST Framework was developed, and a comparable voluntary, risk-based and outcome-based approach to cybersecurity, as a model for this next multistakeholder effort.

---

[40] CTIA, *Mobile Cybersecurity and the Internet of Things: Empowering M2M Communication*, at 18, *available at* http://www.ctia.org/docs/default-source/default-document-library/ctia-iot-white-paper.pdf.

[41] *Id.* at 8 (describing the automation of interconnections between devices).

[42] *Id.* at 13-16.

CTIA and the Automotive Associations further suggest that NTIA initially address several challenges that lend themselves to resolution in the short-term before tackling more complex cybersecurity challenges that will require a more sustained, long-term effort.

Respectfully submitted,

/Thomas Sawanobori/

Robert Strassburger
Vice President, Vehicle Safety and Harmonization

Will Otero
Director, Transportation and Safety Policy

ALLIANCE OF AUTOMOBILE MANUFACTURERS
803 7th Street, NW, Suite 300
Washington, DC 20001
(202) 326-5500

Michael X. Cammisa
Senior Director, Safety

ASSOCIATION OF GLOBAL AUTOMAKERS, INC.
1050 K Street, NW, Suite 650
Washington, DC 20001
(202) 650-5554

Thomas Sawanobori
Senior Vice President, Chief Technology Officer

John Marinho
Vice President, Technology and Cybersecurity

CTIA – THE WIRELESS ASSOCIATION®
1400 16th Street, NW, Suite 600
Washington, DC 20036
(202) 785-0081

Catherine McCullough
Executive Director

INTELLIGENT CAR COALITION
1155 F Street, NW, Suite 1050
Washington, DC 20004
(202) 559-8780

May 27, 2015