TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 N. Courthouse Rd., Suite 200
Arlington, VA 22201 USA
www.tiaonline.org
Tel: +1.703.907.7700
Fax: +1.703.907.7727

July 29, 2013

Via Electronic Filing (incidentcoordination@nist.gov)

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Re: Comments of the Telecommunications Industry Association to the National Institute of Standards and Technology's *Computer Security Incident Coordination (CSIC): Providing Timely Cyber Incident Response* (Docket No.: 130417383-3383-01)

I. Introduction and Statement of Interest

The Telecommunications Industry Association ("TIA") hereby submits comment on the National Institute of Standards and Technology ("NIST") on its request for information relating to Computer Security Incident Coordination ("CSIC") to inform the drafting of a new NIST Special Publication ("SP") to help Computer Security Incident Response Teams ("CSIRTs") to coordinate effectively when responding to computer security incidents.[1] Below, we urge NIST to (1) acknowledge in the new SP that increased certainty in the area of liability is directly correlated to incentivizing enhanced timely information sharing during computer security events; (2) ensure that in its drafting of this new SP, that that ability of organizations to innovate and flexibly address cyber attacks and related issues; and (3) answer select questions in the RFI appropriate for TIA as a representative of hundreds of organizations.

[1] NIST, *Computer Security Incident Coordination; Providing Timely Cyber Incident Response*, 78 Fed Reg 38949–38951 (Jun. 28, 2013) ("RFI").

TIA represents approximately 500 ICT manufacturer, vendor, and supplier companies and organizations in standards, government affairs, and market intelligence. Numerous TIA members are companies producing ICT products and systems, creating information security-related technologies, and providing ICT services information systems, or components of information systems. These products and services innovatively serve many of the sectors directly impacted by the planned NIST SP which will identify technical standards, methodologies, procedures, and processes that facilitate prompt and effective responses to computer security incidents. Representing our membership's commitments in the area of ICT products and services, TIA holds membership and are actively engaged in key public-private efforts that contribute to secure information systems, including the Communications Sector Coordinating Council ("CSCC")[2] and the Federal Communications Commission's ("FCC") Communications Security, Reliability and Interoperability Council ("CSRIC").[3] TIA also actively convenes its members to address issues related to providing timely cyber incident responses in its Cybersecurity Working Group, which has released cybersecurity policy recommendations for critical infrastructure and the global supply chain that have shaped our views below, and that we urge NIST to review,[4] and has filed on numerous cybersecurity-related matters that have addressed this topic previously.[5] TIA also has previously provided NIST with a non-exclusive list of standards, guidelines, best practices, and tools are used by ICT manufacturers and the owners & operators of telecommunications networks to understand, measure, and manage risk at the management, operational, and technical levels.[6]

---

[2] *See* http://www.commscc.org/.

[3] *See* http://transition.fcc.gov/pshs/advisory/csric/.

[4] TIA, *Securing the Network: Cybersecurity Recommendations for Critical Infrastructure and the Global Supply Chain* (Jul. 2012), *available at* http://www.tiaonline.org/sites/default/files/pages/TIA%20Cybersecurity%20White%20Paper-Critical%20Infrastructure%20%26%20Global%20Supply%20Chain_0.pdf#overlay-context=policy/white-papers (TIA Cybersecurity Whitepaper).

[5] *See* https://www.tiaonline.org/policy/cybersecurity.

[6] *See* TIA Comments to NIST, Developing a Framework To Improve Critical Infrastructure Cybersecurity (Docket Number 130208119–3119–01) (Apr. 8, 2013) at 14-16, *available at* http://www.tiaonline.org/sites/default/files/pages/TIA_Comments_NIST_Cybersecurity_Framework_040813.pdf.

In addition, a major function of TIA is the writing and maintenance of voluntary industry standards and specifications, as well as the formulation of technical positions for presentation on behalf of the United States in certain international standards fora. TIA is accredited by American National Standards Institute (ANSI) to develop voluntary industry standards for a wide variety of telecommunications products and sponsors more than 70 standards formulating committees. These committees are made up of over 1,000 volunteer participants, including representatives from manufacturers of telecommunications equipment, service providers and end-users, including the United States government. The member companies and other stakeholders participating in the efforts of these committees and sub-groups have produced more than 3,000 standards and technical papers that are used by companies and governments to produce interoperable products around the world.[7]

TIA's standards development activities have both a national and global reach and impact. TIA is one of the founding partners, and also serves as Secretariat for 3GPP2 (a consortium of five SSOs in the U.S., Japan, Korea, and China with more than 65 member companies) which is engaged in drafting future-oriented wireless communications standards.[8] TIA also is active in the formulation of United States positions on technical and policy issues, administering four International Secretariats and 16 U.S. Technical Advisory Groups (TAGs) to international technical standards committees at the International Electrotechnical Commission (IEC). Finally, TIA is a founding member of the oneM2M, an international partnership that is working to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide.[9]

---

[7] TIA publishes an annual report that includes the latest actions taken by each respective TIA engineering committee toward the development of standards for the advancement of global communications. *See* TIA, Standards & Technology Annual Report (2012), *available at* http://www.tiaonline.org/standards_/about/documents/STAR_2012_Web.pdf. TIA standards are available from IHS, Inc. *See* http://www.ihs.com/.

[8] *See* http://www.3gpp2.org/Public_html/Misc/AboutHome.cfm.

[9] *See* http://onem2m.org/.

II. General Viewpoints on the Need for Improved Information Sharing as Part of Incident Coordination

Many organizations across the public and private sector support the sharing of information in response to computer security incidents, and recognize how important it is to addressing emerging threats in as efficient a way as possible. Though most organizations participate at some level, there is a need to improve the degree to which and how this important threat, vulnerability, or incident information is shared. The current system includes shortcomings which include requiring parties to take burdensome actions to alleviate potential legal issues, as well as related concerns over what happens to data once it is shared with a Federal agency.

Lacking the capability to efficiently share crucial and timely cybersecurity data and information while ensuring strong privacy protections is certainly one of the greatest challenges to improving cybersecurity practices across critical infrastructure. TIA encourages NIST and other Federal actors to eliminate major obstacles to information sharing and to facilitate cooperation in defense against cyber attacks.[10] The current SP addressing incident coordination simply recommends that organizations consult with their legal department before initiating any coordination efforts.[11] We suggest that NIST acknowledge in the new SP that increased certainty in the area of liability is directly correlated to incentivizing enhanced timely information sharing during computer security events.

NIST is undertaking the drafting of this new NIST SP to supplement the existing NIST incident handling guide,[12] SP 800-61, "by significantly expanding the guidance on coordination and information sharing (section 4 of SP 800-61)," with a focus on the coordination aspects of

---

[10] For example, TIA has supported the Cyber Intelligence Sharing Protection Act (H.R. 3523), while appreciating efforts to ensure that an information sharing regime appropriately addresses privacy and civil liberties concerns. *See* Letter from Grant Sieffert, President, TIA, to U.S. House of Representatives Leadership (Apr. 18, 2012), available at http://www.tiaonline.org/sites/default/files/pages/TIA_Letter_to_Speaker_Boehner_and_Leader_Pelos_4_18_12.pdf.

[11] *See* http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf at 4.1.2 (pg. 47).

[12] *See* http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf.

incident response.[13] This new SP will be required of Federal agencies' non-national security systems,[14] and a recommendation to other public and private organizations. As NIST is aware, it and a number of other Federal agencies are in the midst of implementing the President's cybersecurity-themed Executive Order[15] and related Presidential Policy Directive.[16] A key effort under both of these important directives is to improve information sharing mechanisms. In addition, aside from the US-CERT-based system there are numerous public-private partnerships that can be utilized and enhanced to safeguard critical infrastructure through timely sharing of threat information, including the National Coordination Center/Communications Information Sharing and Analysis Center ("NCS/ISAC"), the National Cybersecurity and Communications Integration Center ("NCCIC"), the Partnership for Critical Infrastructure Security ("PCIS"), the Control Systems Security Program ("CSSP"), the Communications Coordinating Council, the IT Coordinating Council, the Network Security Information Exchange, the Cross-Sector Cyber Security Working Group ("CSCSWG"), the FCC's CSRIC, and the National Security Telecommunications Advisory Committee ("NSTAC"). We therefore request that NIST work with its Federal colleagues to carefully ensure that this new SP does not run counter to or conflict with other information sharing systems, be they public, private, or hybrid, in development.

NIST should also ensure that its recommendations enable the flexibility and the ability to innovate. When forming recommendations that are intended to move across sectors, the danger inherently exists to overgeneralize in recommendations. Information-sharing and security partnership platforms differ extensively in competences and their level of development. TIA believes that where recommendations in the SP do cross sectors, an utmost concern for NIST should be to allow specific sectors to continue to innovate to address specific

---

[13] *See* RFI at 38949.

[14] *See* Federal Information Security Management Act (FISMA), Public Law 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate Federal officials exercising policy authority over such systems.

[15] *See* Executive Order 13636 – Improving Critical Infrastructure Cybersecurity, rel. Feb. 12, 2013 ("EO").

[16] *See* Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience, rel. Feb. 12, 2013 ("PPD-21")

threats. We believe that this will be a challenge that can be worked out through a transparent and inclusive process overseen by NIST. For this reason TIA applauds NIST for accepting comment before drafting the SP, and then re-seeking comment once the SP has been drafted.

III. Answers to Select Questions Posed in the RFI

While some of the questions in the RFI are organization-specific and are therefore not appropriate for TIA to answer. However, we provide answers to the following:

General Incident Coordination Considerations

1. *What does your organization see as the greatest challenge in information sharing throughout the incident response lifecycle?*

TIA views the greatest challenge in information sharing throughout the incident response to be uncertainty as to legal repercussions and associated concerns about security of data shared. TIA members have concerns regarding the accidental release of sensitive threat information and its distribution, based on potential legal consequences. Lacking needed certainty as to what can be shared can result in delayed or nixed sharing with important partners.

In addition, we note that many times cyber attack information is of high value to those looking to exploit organizations, and threats are constantly evolving based on responses. In addition, based on liability concerns it is far from instantaneous when organizations to attain in-house legal consent, adding cost and complication (this process is typically required for each occurrence or new partner).

TIA encourages NIST and other Federal actors to eliminate major obstacles to information sharing and to facilitate cooperation in defense against cyber attacks.[17] While the current SP addresses incident coordination by simply recommending that organizations consult with their legal department before initiating any coordination efforts,[18] TIA urges NIST to acknowledge in

[17] For example, TIA has supported the Cyber Intelligence Sharing Protection Act (H.R. 3523), while appreciating efforts to ensure that an information sharing regime appropriately addresses privacy and civil liberties concerns. *See* Letter from Grant Sieffert, President, TIA, to U.S. House of Representatives Leadership (Apr. 18, 2012), available at http://www.tiaonline.org/sites/default/files/pages/TIA_Letter_to_Speaker_Boehner_and_Leader_Pelos_4_18_12.pdf.

[18] *See* http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf at 4.1.2 (pg. 47).

the new SP that increased certainty in the area of liability is directly correlated to incentivizing enhanced timely information sharing during computer security events.

6. *What are the relevant international, sector-specific or de facto standards used or referenced by your organization to support incident handling and related information sharing activities?*

TIA urges NIST to ensure that the new SP reflects the priority for U.S.-based technologies' continued success in the global marketplace which has been enabled through the development of internationally-used standards and best practices. For example, relevant standards include the ISO/IEC 27000-series, which provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system.

Coordinated Handling of an Incident

6. *Do you participate in an incident coordination community such as the Defense Industrial Base (DIB), the Defense Security Information Exchange (DSIE), or an Information Sharing and Analysis Center (ISAC)? What are the benefits? Are there any pain points?*

TIA believes that efforts to improve cybersecurity should leverage public-private partnership-based incident coordination efforts as effectives tool for collaboration on addressing current and emerging threats. Public-private partnerships have been recognized as the basis for the cyber defense of critical infrastructure and cybersecurity policy for the last decade.[19] The success of critical infrastructure owners and operators in preventing progressively complicated attacks has stemmed from the voluntary, public-private model in use because this model is able to evolve in response to changes in threats to critical infrastructure and the risk environment.

[19] *See* Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, 18 (2009) *available at* www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

As both the complexity and number of attacks grow, it will be critical that NIST and other United States government agencies leverage and augment existing public-private partnerships.

Specifically, TIA members as enablers of communications for all sectors, participate in the ISACs, and find them to be a preferable venue because the groups allow for the establishment of trusted relationships by critical infrastructure owners and operators, to include an all-hazards, approach, and to make sector-specific threat determinations. In addition to the ISAC's, relevant public-private organizations that aid in the sharing of computer security threat information include, and in which TIA members engage, include but are not limited to:

- National Coordination Center/Communications Information Sharing and Analysis Center
- National Cybersecurity and Communications Integration Center
- Partnership for Critical Infrastructure Security
- Control Systems Security Program
- Communications Coordinating Council
- IT Coordinating Council
- Network Security Information Exchange
- Cross-Sector Cyber Security Working Group
- FCC's Communications Security, Reliability and Interoperability Council
- National Security Telecommunications Advisory Committee

7. *How do regulatory requirements affect your organization's ability or willingness to share information or collaborate during an incident?*

Generally, TIA members view regulatory requirements to discourage timely sharing of critical information because such requirements create inflexible and, as time passes, outdated reporting structures and give rise to potentially serious liability risks. Currently, a number of national-level cybersecurity-related reporting requirements already exist (see below), some of which overlap, and this can lead to serious risks for organizations where one agency may use information shared in an ISAC to pursue a regulatory violation such as HIPPA or the SEC's disclosure requirements. Other parties interested in pursuing criminal or civil charges may also use this information. We understand this issue will likely need to be addressed in Congress to be resolved.

8. *What regulatory bodies are you required to report information to regarding incidents? For each regulatory body, what kind of information does your organization report and what has been your organization's reporting experience?*

TIA cannot speak to any individual organization's experience, but we do note that a number of national-level cybersecurity-related reporting requirements already exist, including:

Agency	Rule/Threshold
FCC	Wireline, wireless, cable, and satellite communications service providers, including interconnected Voice over Internet Protocol ("VoIP") service providers, must submit reports in the event that certain network outages reach the specified criteria and thresholds through the FCC's Network Outage Reporting System ("NORS").
FTC	Vendors of personal health records and related entities to notify consumers when the security of their individually identifiable health information has been breached.
FTC	Any financial institution that provides financial products or services to consumers must give consumers privacy notices that explain the institutions' information-sharing practices.
FTC	Requires companies to get parental approval before collecting online information from children under 13 years of age.
FERC	Electric utilities operating bulk power system assets must comply with eight North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP") standards.
HHS	Following a breach of unsecured protected health information, Health Insurance Portability and Accountability Act-covered entities must provide notification of the breach to affected individuals, the HHS Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities that a breach has occurred.
OMB/ DHS	Federal agency Chief Information Officers ("CIOs"), Inspectors General, and the Senior Officials for Privacy must submit to DHS' Federal Network Resilience division via CyberScope: (1) data feeds directly from security management tools; (2) government-wide benchmarking on security posture; and (3) agency-specific interviews.
SEC	Publicly traded United States companies must report information that is considered to have a substantial likelihood that a reasonable investor would consider it important in making an investment decision or if the information would significantly alter the total mix of information made available.

Coordinated Handling of an Incident

1. *What, if any, types of information would create risk or disadvantage if shared by your organization?*

As mentioned above, unless liability issues are resolved, the legitimate disclosure of timely threat information in the US-CERT system can give rise to serious liability for a company, be it regulatory, criminal, or civil. Information shared accidentally can generally damage an organization and lead to the same liability.

3. *What types of protections, redactions, or restrictions would aid your organization in sharing information?*

As described above, liability must be addressed to provide organizations with increased legal certainty. This key step would have immediate and positive impacts on the sharing of important threat information.

6. *What incentives exist for your organization to share information with other organizations during an incident?*

Efficient distribution of timely data between and among public and private organizations related to cyber attacks and susceptibilities is a widely-recognized necessity for improving cybersecurity generally. It allows for more informed approaches to computer security events at increased speed, benefitting both national security and business continuity.

7. *What disincentives exist that might prevent your organization from sharing information with other organizations during an incident?*

I. As described above, legal liability issues surrounding information sharing serve as the largest disincentive to engagement in this area.

IV. Conclusion

TIA thanks NIST for its public request for input on this new SP, and the ICT manufacturing and vendor community stands ready to work with NIST as it moves forward.

Respectfully submitted,

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

By: */s/ Danielle Coffey*

Danielle Coffey
Vice President & General Counsel, Government Affairs

Dileep Srihari
Director, Legislative & Government Affairs

Brian Scarpelli
Senior Manager, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
10 G Street N.E.
Suite 550
Washington, D.C. 20002
(202) 346-3240

July 29, 2013