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 8, 2013

Via Electronic Filing

Lisa Barr
DHS/NPPD/IP/Office of Strategy and Policy
245 Murray Lane, SW, Mail Stop 8530
Arlington, VA 20598-8530

Re: Comments of the Telecommunications Industry Association to the Department of Homeland Security's National Protection and Programs Directorate on *Review and Revision of the National Infrastructure Protection Plan* (Docket Number DHS-2013-0024)

I. Introduction and Statement of Interest

The Telecommunications Industry Association ("TIA") hereby submits comment on the Department of Homeland Security ("DHS") National Protection and Programs Directorate's ("NPPD") request for information[1] to inform its review of the 2009 National Infrastructure Protection Plan ("NIPP")[2] to conform to the requirements of Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* ("PPD-21").[3] TIA appreciates the need for the NPPD to maintain a comprehensive and evolved risk management framework that incorporates DHS; the Sector-Specific Agencies ("SSAs"); other Federal departments and agencies; state, local, tribal, and territorial governments; critical infrastructure owners and operators; and other stakeholders in industry, academia, and non-governmental organizations. We agree that the NIPP has a key role in protecting critical infrastructure moving forward.

---

1 DHS, *Review and Revision of the National Infrastructure Protection Plan*, Notice and request for comments, 78 Fed. Reg. 34112–34115 (Jun. 6, 2013) ("RFC").

2 NIPP, *available at* www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

3 Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience, rel. Feb. 12, 2013.

Below, in our responses to the questions posed by NPPD in the RFC, we urge that NPPD proceed in its implementation of PPD-21 guided by the following principles: (1) that successful efforts to improve cybersecurity will leverage public-private partnerships to effectively collaborate on addressing current and emerging threats; (2) that the U.S. government should enable and stimulate greater cyber threat information sharing between the public and private sector; (3) that policymakers and regulators should ensure that they address economic barriers for owners and operators of critical infrastructure in efforts to secure cyberspace; (4) that Federal research funding for ICT and specifically cybersecurity research and development should be prioritized; (5) that the global nature of the information and communications technology ("ICT") industry necessarily requires a global approach to address cybersecurity concerns; and (6) that a global supply chain can only be secured through an industry-driven adoption of best practices and global standards.

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 PPD-21 and the accompanying Executive Order 13636.[4] Representing our membership's commitments in this area, we hold membership and are actively engaged in key public-private efforts that contribute to secure information systems, including the Communications Sector Coordinating Council ("CSCC")[5] and the Federal Communications Commission's ("FCC") Communications Security, Reliability and Interoperability Council ("CSRIC").[6] TIA also actively convenes its members to address issues related to the EO and PPD-21 in its Cybersecurity Working Group, and has released cybersecurity policy recommendations

---

4 Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, rel. Feb. 12, 2013 ("EO").

5 *See* http://www.commscc.org/.

6 *See* http://transition.fcc.gov/pshs/advisory/csric/.

for critical infrastructure and the global supply chain that have shaped our views below, and that we urge NIST to review.[7]

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.[8]

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.[9] 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,

---

[7] 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).

[8] 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/.

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

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.[10]

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

II. TIA Input on Issues To Be Addressed in the Successor to the NIPP

In the RFC, NPPD notes a number of changes that it intends to make to the NIPP pursuant to PPD-21, and specifically requests input on several aspects. We are limiting our input below to the areas where NPPD has requested input.

Updates to Information-Sharing Tools and Mechanisms

NPPD requests comments and input on ways that the current NIPP information-sharing approach and mechanisms could be changed and improved.[11] Providing 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 NPPD to eliminate major obstacles to information sharing and to facilitate cooperation in defense against security and cybersecurity attacks.

The current NIPP "network approach" to information sharing, stating that this model allows distribution and access to information both vertically and horizontally, as well as the ability to enable decentralized decision-making and actions.[12] This approach is realized by the Homeland Security Information Network ("HSIN"), composed of multiple, non-hierarchical communities of interest ("COIs") that offer CIKR partners the means to share information based on secure access. As far back as 2007, the Government Accountability Office found that the HSIN did not develop a comprehensive inventory of key state and local information-sharing initiatives, creating the risk that "effective information sharing is not occurring and that HSIN may be duplicating state and local capabilities."[13] While we understand that HSIN has evolved and

---

[11] RFC at 34114.

[12] *See* NIPP at 56.

[13] See GAO, *Information Technology: Homeland Security Information Network Needs to Be Better Coordinated with Key State and Local Initiatives*, GAO-07-822T (May 10, 2007).

improved much since 2007, we suggest that the NIPP continue to strive to ensure that it coordinates with state and local activities so that efforts are not duplicated.

Critical Infrastructure Security and Resilience Regulatory Programs

TIA appreciates NPPD's effort to better integrate existing regulatory programs into the NIPP framework, without proposing new regulatory authority.[14] We believe that the updated NIPP should do so where appropriate.

NPPD revisions to the NIPP should continue to encourage the leveraging of public-private partnerships as an effective tool for collaboration on addressing current and emerging security and cybersecurity threats. Public-private partnerships have been recognized as the basis for the cyber defense of critical infrastructure and cybersecurity policy for the last decade.[15] 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. 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. We note that the 2009 NIPP already describes the benefits of the public-private partnership; [16] this should be maintained in the successor to the NIPP.

In sum, TIA strongly believes that the public-private partnership model for cybersecurity achieves what mandatory requirements cannot: (1) collaboration and cooperation instead of compliance in lieu of penalty; (2) an elastic and cohesive method to confront cyber attacks; and (3) prevention of duplicative and expensive requirements, permitting assets to be concentrated on protection rather than outmoded mandates.

---

[14] RFC at 34114.

[15] 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.

[16] National Infrastructure Protection Plan, i-8 (2009) *available at* www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

Between the NIPP and many other efforts, there are numerous public-private partnerships that can be utilized and enhanced to safeguard critical infrastructure, 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"). These and other public-private partnerships should continue to serve as a foundational principle in the NIPP.

Based on the above, TIA recommends that in its revisions to the NIPP, NPPD ensure that the NIPP continue to concentrate its efforts on improving public-private partnerships, as they have demonstrated themselves as effective means in giving industry required flexibility to prevent attacks, and to specifically avoid effectually constructing a new regulatory regime. This approach is the most effective way to gather broad and cross-cutting stakeholder input on the regulatory requirements across sectors that will inform this effort by NPPD in its NIPP revisions.

The successor to the NIPP should ensure that it maintains the needed flexibility and the ability to innovate for the ICT manufacturers. When forming recommendations that are intended to move across sectors, the danger inherently exists to overgeneralize in recommendations. For the successor to the NIPP, an utmost concern for DHS should be to allow specific sectors to continue to innovate to address specific threats. We believe that this will be a challenge that can be worked out through a transparent and inclusive process overseen by NIST.

Currently, "critical infrastructure" sectors affected by the EO include energy, agriculture/food, information technology, banking/finance, telecommunications/broadcasting, commercial services, defense industrial base, chemical, dams, health care, water, nuclear, critical

manufacturing, transportation; and postal/shipping. These sectors have been identified by DHS pursuant to Presidential Policy Directive #7, which established US cybersecurity policy in 2003.[17] Under the EO, not later than July 12, 2013, the Secretary of Homeland Security ("Secretary") shall identify critical infrastructure where a cybersecurity incident could result in catastrophic regional or national effects on public health or safety, economic security, or national security, using a consultative process and drawing on the expertise of the Sector Specific Agencies ("SSAs") designated in PPD-21. Per the EO, DHS is the SSA for communications. The EO, however, prohibits, the Secretary from identifying "any commercial information technology products or consumer information technology services" under this process. TIA supports the inclusion of this crucial prohibition that will help ensure that the manufacturers and suppliers of such commercial information technology products have the needed flexibility to innovate. So long as DHS, in fulfilling its responsibilities surrounding the identification of critical infrastructure, does not stifle the ability of the manufacturers of the ICT equipment that enables each of the critical infrastructure sectors to innovate, and instead relies on each sector member to determine their needs through the ICT they comprise their service of, we believe that the Framework can embody the necessary flexibility for effective cybersecurity across sectors.

The necessity of international approaches and standards. TIA believes that the current NIPP appreciates the needed 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. We urge NPPD to ensure that the successor to the NIPP continues to recognize that that the global nature of the ICT industry necessarily requires a global approach to address cybersecurity concerns, and that a global supply chain can only be secured through an industry-driven adoption of best practices and global standards. Any approach taken in the successor to the NIPP must involve international cooperation and heavy engagement with the private sector but should not include language that might put the government in a position to determine the future design and development of technology. TIA

[17] Presidential Policy Directive/PPD-7, National Terrorism Advisory System (NTAS), rel. Jan. 16, 2011.

believes that the United States should work with other governments to establish international security standards in order to prevent hobbling United States industry with United States-only standards. We are concerned about the impact on our nation's global competiveness as well as technology innovation and development of having the United States government set specific technical standards. Neither the successor to the NIPP nor any other government action should enact cybersecurity policies that would restrict trade in telecommunications equipment imported to, or exported from, other countries that are part of the global trading system. While other countries cite similar concerns regarding foreign ICT equipment and are currently considering trade restrictive measures, we believe that the U.S. should be a leader is this area: TIA recommends that the U.S. government exercise extreme caution in how it approaches this issue since U.S. policy will effectively serve as a global standard. If the U.S. develops unique approaches that have the effect of restricting trade unnecessarily, U.S. global economic competitiveness could be severely affected by other export markets adopting similar restrictive policies. In short, a global industry necessarily requires a global approach to address cybersecurity concerns.

The successor to the NIPP should reflect the important role that non-mandatory best practices have in increasing communications network resiliency and security, along with supply chain integrity. In practice, best practices are not "created," but are recognized by stakeholders through information sharing activities as already widely-used effective means to address issues. Given the fact that each best practice is not relevant for each area, sector, node, etc. of the communications industry, because they are not mandated, network operators are allowed for the flexibility to employ the best equipment and systems that meets their specific challenges to network reliability. In addition, best practices allow for the "co-existence of new and old technologies"[18] and therefore help facilitate the smoothest transitions in technology deployments. There are currently numerous voluntary industry efforts underway that continually formulate, aggregate, and update best practices, and network operators and equipment vendors regularly look to best practices, both internal and external to their

[18] CSRIC Working Group 6, *Final Report: Best Practices Implementation* (rel. Dec. 2010) at 3.

organization, notably the FCC CSRIC's Cyber Security Best Practices Working Group.[19] We strongly urge NPPD to incorporate the importance of best practices into the successor to the NIPP, and use the same to promote the development of further best practices within, and where appropriate, across sectors.

Updates on Measurement and Reporting Processes and Risk-Informed Resource Allocation

TIA congratulates NPPD on its continued work with SSAs to improve metrics and reporting processes to assess national critical infrastructure security and resilience efforts and identify opportunities for improvement. While NPPD does not appear to be seeking input on ways to further improve the NIPP regarding measurements and reporting processes and risk-informed resource allocations past the intra-governmental consultations it notes, TIA encourages NPPD in its NIPP revisions to promote increased interaction with the SCCs and private sector owners and operators of critical infrastructure, as well as SSAs.

Closer Integration of Physical and Cyber Security

DHS requests comments on the timeframe and requirements for research, development, and incentives for increased cyber-physical integration and how the successor to the NIPP can integrate the concepts and implementation of physical and cybersecurity.[20] The Interagency Task Force, through its working groups,[21] has a very important and highly complex responsibility. Representing the ICT manufacturer and vendor community, TIA and its members concur that critical infrastructure, both physical and cyber, is a key element of our national security and economic prosperity, and it is at risk from a variety of hazards, including cyber attacks. We actively seek out ways to participate in the Interagency Taskforce's working groups

---

[19] We note that the CSRIC has specifically addressed cybersecurity best practices, including those which address general "hygiene," and a recommended approach to cyber attacks, amongst many others which the Framework should incorporate. *See* CSRIC Working Group 2A, *Cyber Security Best Practices, Final Report*, (Mar. 2011), *available at* http://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf.

[20] RFC at 34114-34115.

[21] *See* http://damsafety.org/media/Documents/Security/ITF%20Fact%20Sheet%20March%202013.pdf.

to address physical and cybersecurity threats. We encourage DHS to more proactively engage the private sector in a public and transparent manner. Noting our support for the formalized public-private partnerships in the critical infrastructure sectors with SSPs and SCCs already in the 2009 NIPP, we have found a number of the DHS consultations through its various work groups which aim to implement PPD-21 and the EO to be inadequately noticed to stakeholders, and at times little more than readouts of planned activity with modest solicitation for feedback. Specifically, we believe that (1) the meetings held by these WGs should be more widely announced, through such means as the Federal Register; and (2) these WGs should have sought more written input via public consultations from stakeholders. Though DHS may not be required to seek this input and deadlines are tight on DHS and other agencies, such a step would increase transparency in the process and increase awareness of important issues throughout affected communities. While some conversations involve privileged and/or company-specific information, we believe that the public consultation role valuable in many circumstances particularly the closer integration of physical and cybersecurity, and has been underused by DHS.

TIA believes that end-user education is also a crucial aspect to improving both physical and cyber threat ecosystem response capabilities, as many vulnerabilities are already known and related attacks are relatively easily preventable. Numerous efforts exist across sectors to inform end users of proper steps to take to ensure that proper cyber "hygiene" is impressed. We support the CSRIC-based recommendation that network operators and service providers educate the customers on important steps that should be taken, from the use of adequate passwords to encryption of data.[22] With this in mind we specifically support the successor to the NIPP including emphasis on the importance of both physical and cyber "hygiene."

In a separate but related response, TIA has provided detailed comments on existing and desired incentives to improve cybersecurity practices,[23] which we urge NPPD to consider in drafting the

[22] *See* CSRIC Working Group 2A Report.

[23] *See* https://www.tiaonline.org/sites/default/files/pages/TIA-Comments-NIST-NTIA-Cybersecurity-Framework-Incentives-042913.pdf.

successor to the NIPP. Existing incentives include public-private partnership; standards and best practices; and competitive differentiation and business continuity. Desired incentives include maintaining the ability to innovate and to flexibly meet goals; enhanced information sharing; and increasing Federal cybersecurity research and development; among others. TIA believes that the integration of physical and cyber security needs will be organically be promoted by maintaining an emphasis on these important concepts in the successor to the NIPP. In addition, Federal recognition of security processes and practices certified and accredited by recognized standards bodies would also serve as an effective incentive.

Review of the Risk Management Approach

In the RFC, NPPD states that it does not intend to make significant changes to the basic structure and concept of the risk management framework but rather to review how PPD-21 and other recent directives and events will influence the context and application of the risk management framework going forward.[24] TIA believes that the consultative approach prescribed by the NIPP is the correct framework, and supports such an approach by NPPD.

ICT manufacturers and vendors who enable each critical infrastructure sector to function and to communicate with other entities. In that context, defining and assessing risks generally and for the purposes of cybersecurity is a unique evaluation that considers numerous factors that may help or hurt the network, including software, hardware, human, and inter-government relationship factors.[25] Other important factors include those noted in the 20 Critical Controls,[26] all of which were recently determined by the FCC's CSRIC to be applicable to the enterprise communications networks.[27]

---

[24] RFC at 34115.

[25] *See* NSTAC, *Next Generation Networks Task Force Report* (rel. Mar. 28, 2006) at G-1 to G-10.

[26] *See* http://www.sans.org/critical-security-controls/.

[27] *See* CSRIC Working Group 11, *Consensus Cyber Security Controls, Final Report*, (Mar. 2013) at Appendix 6, *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG11_Report_March_%202013.pdf.

What is important for NPPD to consider as it looks to the successor to the NIPP are these values that, as NPPD notes in the RFC, are agreed upon by all stakeholders. PPD-21 requires DHS to quickly complete a number of important determinations and deliverables, but the fundamentals of the NIPP – namely recognizing and building on existing public and private sector protective programs and resiliency strategies in order to be cost-effective and to minimize the burden on CIKR owners and operators[28] – must not be lost.

[28] NIPP at 1.

III. Conclusion

TIA supports NPPD in its important task of revising the NPPD, and we urge the consideration of the above positions. The ICT manufacturing and vendor community stands ready to work with DHS and all other government actors to improve both physical and cyber security.

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 8, 2013