TIA
ADVANCING GLOBAL COMMUNICATIONS

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 22, 2013

Via Electronic Filing

Keith Bubar
National Institute of Standards and Technology
100 Bureau Drive Mail Stop 1640
Gaithersburg, MD 20899-1640

Re: Comments of the Telecommunications Industry Association to the National Institute of Standards and Technology's *Proposed Establishment of a Federally Funded Research and Development Center* (Docket No.: 130212127-3550-02)

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 proposed establishment of a Federally Funded Research and Development Center ("FFRDC") for the purpose of supporting the mission of the National Cybersecurity Center of Excellence ("NCCoE") by "(1) Research, Development, Engineering and Technical support; (2) Program/Project Management, to include but not limited to expert advice and guidance in the areas of program and project management focused on increasing the effectiveness and efficiency of cybersecurity applications, prototyping, demonstrations, and technical activities; and (3) Facilities Management."[1] Below, we express our support for the creation of the FFRDC to support the NCCoE, and encourage a focus on ensuring that cybersecurity concerns are fully appreciated and understood throughout public entities' processes, and coordination with numerous existing public-private partnerships.

[1] NIST, *Proposed Establishment of a Federally Funded Research and Development Center-First Notice*, 78 Fed Reg 23744 (Apr. 20, 2013) ("Notice").

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.[2] 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")[3] and the Federal Communications Commission's ("FCC") Communications Security, Reliability and Interoperability Council ("CSRIC").[4] 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 for critical infrastructure and the global supply chain that have shaped our views below, and that we urge NIST to review.[5]

In addition, TIA 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] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, rel. Feb. 12, 2013 ("EO").

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

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

[5] 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).

[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. Problems with the Existing State of Cybersecurity Research & Development

While the United States maintains the most resilient research ecosystem across the globe, indications are emerging of wearing away in the ICT sector as other countries continue to make decisive measures to interest investment in ICT research to build innovation-based economies.[10] The resulting effects on the U.S. ICT sector of a less competitive ICT research ecosystem are tangible. As far back as 2009, the National Academy of Sciences stated that "[t]he nation risks ceding IT leadership to other generations within a generation unless the United States recommits itself to providing the resources needed to fuel U.S. IT innovation."[11] TIA maintains that the United States government has not offered or effected the commitment needed to avert this risk: Federal investment in ICT research remains comparatively low when compared to other scientific fields. TIA believes that Federal funding for cybersecurity research and development should be prioritized, and should coordinate research activities amongst contributing agencies, incorporating industry input.

Past the economic costs of other nations bettering the United States in ICT research and development, the most distressing are in the area of national security. We note that this risk is evident to the United States government – the National Critical Infrastructure Security and Resilience R&D Plan emphasizes the changing nature of threats, annual metrics, and other appropriate data being used to ascertain priorities and to help point R&D requirements and investments in the right direction.[12]

[10] TIA, *U.S. ICT R&D Policy Report*, (2011) available at http://www.tiaonline.org/sites/default/files/pages/TIA%20U%20S%20%20ICT%20RD%20Policy%20Report.pdf.

[11] NRC, *Assessing the Impacts of Changes in the Information Technology R&D Ecosystem: Retaining Leadership in an Increasingly Global Environment*, 1 (2009), available at www.nap.edu/catalog/12174.html.

[12] DHS, National Infrastructure Protection Plan (2009), available at http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

III. TIA Supports the Creation of the Proposed FFRDC

NIST seeks comments generally on this proposed FFRDC, and specifically on the proposed scope of work along with existing private- or public-sector capabilities in this area that NIST should consider.[13] TIA supports increased cybersecurity research and development funding, and therefore supports the creation of this FFRDC as proposed by NIST, with the FFRDC's activities being limited to supporting the NCCoE. We believe the the FFRDC's goals proposed in the NIST notice would augment the widespread adoption of integrated cybersecurity, tools, and technologies, particularly the proposal to promote cybersecurity standards, guidelines, and best practices, which we believe the NCCoE can help proliferate through its continued outreach.

The FFRDC should recognize that a large challenge in improving cybersecurity, particularly in the public sector, is ensuring that cybersecurity concerns are fully appreciated and understood throughout public entities' processes. This will require adequate workforce training across the federal government. In addition, TIA believes that end-user education is also a crucial aspect to improving cyber threat ecosystem response capabilities, as many cyber 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 generally educate the customers on important steps that should be taken, from the use of adequate passwords to encryption of data,[14] and encourage this to be a stated purpose in the new FFRDC's scope.

TIA also believes that the FFRDC should fully coordinate with and leverage public-private partnerships as an effective tool for collaboration on addressing current and emerging threats. Public-private partnerships have been recognized as the basis for the cyber defense of critical

[13] *See* Notice at 23745.

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

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, its new FFRDC, and other United States government agencies leverage and augment existing public-private partnerships through the NCCoE.

TIA believes that transitioning from a public-private partnership model to a mandatory regulatory regime, or one that is effectively of a mandatory nature, would have a negative impact on the security of critical infrastructure, and we urge NIST to be conscious of this serious concern as is scopes the FFRDC. 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.

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 critical infrastructure protection.CSRIC, and the National Security Telecommunications Advisory Committee ("NSTAC"). These and other public-private partnerships should serve as the foundation for moving forward with critical infrastructure

[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.

protection, and should factor into NIST's evaluation of existing public- and private-sector capabilities that currently in the formation of the FFRDC, and coordination with these and other groups should be a priority.

IV. Conclusion

TIA supports the proposed creation of the FFRDC to support the mission of the NCCoE. The ICT manufacturing and vendor community stands ready to work with NIST as it moves forward with its solicitation and establishment of the FFRDC.

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 22, 2013