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

Submitted via csfcomments@nist.gov

December 13, 2013

Adam Sedgewick
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

Re: ***Request for Comments on the Preliminary Cybersecurity Framework***

Dear Mr. Sedgewick:

The Telecommunications Industry Association ("TIA")[1] hereby submits input to the National Institute of Standards and Technology ("NIST") on its Preliminary Cybersecurity Framework ("Framework"),[2] towards fulfilling the vision of the President in Executive Order 13636, "Improving Critical Infrastructure Cybersecurity,"[3] for a voluntary, prioritized, flexible, repeatable, performance-based, and cost-effective approach to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.[4] In addition, we have also appended to this TIA's line edits for NIST's consideration. We look forward to working with NIST as February 2014 approaches and the Framework must be finalized. Towards that end, TIA

[1] TIA represents hundreds of information and communication technology ("ICT") manufacturer, vendor, integrator, and supplier companies and organizations in both policy advocacy and American National Standards Institute-accredited standards development. 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 EO and the related Presidential Policy Directive. 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") and Information Technology Sector Coordinating Council ("ITSCC"), and the Federal Communications Commission's ("FCC") Communications Security, Reliability and Interoperability Council ("CSRIC"). TIA also actively convenes its members to address issues related to the EO and PPD-21 in its Cybersecurity Working Group. For more on TIA, please see our Policy Playbook at http://www.tiaonline.org/policy/tia-2013-playbook.

[2] *Request for Comments on the Preliminary Cybersecurity Framework*, Docket No. 130909789-3789-01, 78 FR 64478 (2013).

[3] Executive Order No. 13636, 78 Fed. Reg. 11739 (2013) ("EO").

[4] EO, Sec. 7(b), 8(a).

offers the specific input below based on the consensus views of its hundreds of information and communications technology ("ICT") manufacturer, vendor, and supplier member companies.[5]

NIST Should Clearly Define the Purpose and Nature of the Framework

The Framework is written for an extraordinarily broad audience, which has varying ranges of sophistication in terms of cybersecurity risk management. It includes critical infrastructure owners and operators and the broader community, regulatory agencies governing these organizations, and the international community. We suggest that some additional guidance in the introductory language may be beneficial to all of these audience members. TIA and others have heard the statements from the Administration that the Framework is not intended to either function in effect as a regulation, nor is it intended to result in new regulations on CIKR owners and operators or other stakeholders. However, there is a very real possibility that some agencies may simply transplant the Framework into regulation. To try to prevent new, unnecessary regulations, we request that NIST include language affirmatively stating that Framework is voluntary and reiterating the Administration's commitment that the Framework is not intended to function as a regulation.

It is also very important that NIST be clear on these points because of the international anticipation of this Framework. Numerous regions and countries are looking to the United States for guidance on how to approach cybersecurity solutions. For example, we support the Executive Order's stated deference to internationally-adopted standards and best practices being used as cybersecurity solutions. Clearly expressing this priority in the Framework as well as recognizing that a global supply chain can only be secured through an industry-driven adoption of best practices and global standards (i.e., that the global nature of the ICT industry necessarily requires a global approach to address cybersecurity concerns) will greatly aid foreign governments and organizations in understanding the nature of the Framework. This

[5] For a list of TIA members, see https://www.tiaonline.org/about/member-list.

also highlights a previous point that the voluntary nature of the Framework should be emphasized so that it is not misunderstood as mandatory.

Guidance on the scope, or suggested prioritization in implementation, of the Framework would also be beneficial to all of these audiences. The purpose of the Executive Order was to protect critical infrastructure, and so, NIST should suggest that the highest priority of implementing the Framework should be for those processes and assets directly involved in the delivery of critical infrastructure services. All organizations will be struggling to most effectively allocate their resources as they adopt this Framework, and such guidance would assist companies in focusing on achieving the objectives of the Executive Order. This would in no way limit a company from applying the Framework more broadly, or discourage it from doing so.

NIST Should Ensure the Flexible Nature of the Framework

To ensure adoption it will be crucial that NIST ensure that the document be easy to understand, particularly for the entities that may lack the personnel and resources to dedicate to adoption. Especially with the Framework at such an early phase, NIST should ensure that it is flexible in nature and translatable to maximize the ease in understanding and adoption. Sector-specific approaches that are created by Sector Coordinating Councils and other effective public-private partnership efforts will be key.

Tiers and Profiles

TIA agrees with NIST's previous commitment that numerous sector- and organization-specific factors will determine the appropriate Framework Tier for a given organization. As we represent a wide variety ICT vendors and manufacturers who supply equipment to CIKR owners and operators across the identified CIKR sectors, we are cognizant of the need for owners and operators to determine the tier that is most appropriate for them. We are also cognizant, however, that CIKR owners and operators are likely to require suppliers both to adopt the

Framework and to meet Tier 4 status, whether or not that would be otherwise appropriate for the supplier. Such use, however, is inconsistent with the Executive Order's intention that the Framework be flexible, performance-based, and cost-effective;[6] as well as contrary to the intentions of the Framework that the appropriate Tier may vary by organization and by category and that and the Tiers are a tool to aid an organization in improving its cybersecurity posture rather than a hammer to be used by an outside party, regardless of cybersecurity risk, feasibility of implementation, or other business concerns.

Perhaps more importantly, as there is no methodology for how to calculate and apply Tiers, using the Tiers outside of an organization's risk management process is fraught with the risk of false comparisons between organizations based on non-standard profiles. The same is true for Framework Profiles: the lack of methodology for calculating a Profile makes the external uses contemplated by the Framework in Section 3.3, such as for communicating requirements to external service providers, reporting results, or comparison with acquisition requirements, at best inaccurate as there is no standard for measuring one organizations Framework Profile against other organizations' Framework Profiles.

To avoid reliance on such inaccurate comparisons, TIA asks NIST to clarify that for this version of the Framework, the purpose of Profiles and Tiers is to aid internal risk management processes and that they are not appropriate external metrics. To the extent Profiles and Tiers are used outside an organization, it should be to aid organizations with their internal risk management, *e.g.*, through Sector Coordinating Councils providing illustrative Target Profiles and Tiers as a sample to aid organizations with creating their own Target Profiles. Then, as NIST develops the next version of the Framework, TIA encourages NIST to develop a methodology for calculating and applying Profiles and Tiers so that the results can validly be used for information and comparison outside the organization. In the meantime, the Framework Core provides sufficient common language to aid CIKR owners and operators in expressing needs to external suppliers and service providers, and indeed, would provide a more accurate and

[6] EO, Sec. 7(b).

reliable basis to communicate such needs until the Profiles and Tiers are based on common methodology.

Adoption

As evidenced by the repeated questions at the Fifth Cybersecurity Framework Workshop, industry seeks clarity on a definition of "adoption." To provide this certainty, TIA suggests that NIST incorporate directly into the Framework the definition of "adoption" that it distilled from that workshop:[7]

> *An organization adopts the framework when it uses the Cybersecurity Framework as a key part of its systematic process for identifying, assessing, prioritizing, and/or communicating:*
> - *cybersecurity risks,*
> - *current approaches and efforts to address those risks, and*
> - *steps needed to reduce cybersecurity risks as part of its management of the organization's broader risks and priorities.*

Incorporating this consensus definition directly into the Framework is even more important because of the real possibility that agencies will incorporate the Framework into regulations. Without clear language in the Framework itself expressing what constitutes adoption, agencies unfortunately may turn the Framework's guidance into broad-ranging, strictly prescriptive requirements that will not enable the type of flexibility needed for organizations of different sizes and of differing relationship to critical infrastructure.

Duplication of Effort

We do not believe that NIST has the goal of creating a new certification regime for suppliers that would run parallel to existing efforts and that would serve simply add cost to the risk management steps that suppliers already undertake, and – particularly in the case of the

[7] NIST, *Update on the Development of the Cybersecurity Framework* (Dec. 4, 2013), available at http://www.nist.gov/itl/upload/nist_cybersecurity_framework_update_120413.pdf.

existing efforts which already surpass the Framework's recommendations – would not in reality increase resiliency to cyber-based attacks. So, TIA also asks NIST to clarify in the introduction that organizations whose existing cybersecurity programs already accomplish what the Framework outlines may not need to do anything else to be considered to have "adopted" the Framework.

NIST Should Carefully Consider its Proposed Appendix B (Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program)

The privacy appendix is an important aspect of this Framework, as the Executive Order makes clear. We appreciate NIST's effort to ensure that consumer privacy is protected as organizations take steps to improve their resiliency to cyber-based attacks. In the past, TIA has noted its support of efforts to ensure that an information sharing regime appropriately addresses privacy concerns.[8]

As with other aspects of the Framework, NIST should place appropriate language into the Framework to make clear that it does not intend to impose burdensome regulations that would detract from dynamic voluntary efforts to address privacy concerns in standardization efforts and public-private partnerships. This is important for the organizations which are the target audience of the document, the organizations they interact with, and foreign governments.

NIST should also take great care that Appendix B is tailored to implement the Framework's clearly-defined objectives. As written, some aspects of Appendix B address the general implementation of privacy policies, not just those implicated by activities relating to assessing and responding to cyber threats. For example, Appendix B's methodology directs

[8] *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.

organizations to identify all personally-identifiable information ("PII") of "employees, customers, or other individuals that they collect or retain, or that may be accessible to them," while it is not clear how such an inventory that does not address other types of important information related to cybersecurity is directly linked to the goals of the Framework. NIST should also ensure that its Appendix B be appropriately tailored to be specific to the Framework. TIA appreciates that NIST has worked to link Appendix B to the Framework Core and we urge NIST to look critically at Appendix B with this goal in mind.

As with the Framework's tiers, we believe this illustrates why it would be prudent for NIST to pull back on this Appendix and more carefully approach it in the version 2.0 of the Framework. If the Appendix is included in this first version of the Framework, TIA asks that NIST consider the alternative approach recently filed on behalf of several industry sectors. [9] Whether retained in the version 1.0 of the Framework or left to version 2.0, TIA urges NIST to consider a more appropriately tailored Appendix B based on separate, formal consultations with privacy stakeholders.

NIST's Compendium of Standards

Originally, NIST undertook an effort to collect existing standards toward building a Compendium which would provide a list of standards applicable to risk management for one or more sectors. TIA, among many other organizations, submitted potential standards to that Compendium which were accepted by NIST, and we have since identified several others in the public safety communications space that we believe should be considered for inclusion.[10] NIST has indicated that it will not be moving forward with the previously-issued Compendium. It is consistent with the Executive Order and crucial to what TIA believes is the ultimate goal of the

[9] For example, alternative approaches reflecting consensus private sector practices have already been proposed to NIST. *See* Alternative Privacy Methodology to Protect Privacy for a Cybersecurity Program, attached to letter from Harriet Pearson, Hogan Lovells US LLP to Adam Sedgewick, Information Technology Laboratory, National Institute of Standards and Technology (Dec. 5, 2013), *available at* http://csrc.nist.gov/cyberframework/framework_comments/20131205_harriet_pearson_hoganlovells.pdf.

[10] *See* Attachment A to this document.

Framework – increased widespread resiliency to cyber-based attacks – that awareness of these standardization and best practice efforts that the Framework is built on be increased. For this reason we believe that NIST should not abandon the Compendium effort.

***

TIA appreciates this opportunity for input on the Framework. We urge you to consider the above and the attached line edits, and to contact the undersigned with any questions.

Respectfully submitted,

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

By: */s/ Danielle Coffey*
Danielle Coffey
Vice President, Government Affairs

Brian Scarpelli
Senior Manager, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 North Courthouse Road
Suite 200
Arlington, VA 22201
703.907.7700

December 13, 2013

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

Attachment A: Further TIA Standards for Inclusion in NIST Preliminary Framework Compendium

Standard Name	Standard Description
TIA-102.AAAB-A, "Project 25 Digital Land Mobile Radio - Security Services Overview"	A general land mobile radio communications system consists of subscriber units, base stations, fixed equipment for single-site to wide area operation, console operator positions, and computer equipment. The subscriber units include portable radios for handheld operation and mobile radios for vehicular operation. The base stations are for geographically fixed installations. Other fixed equipment is used for wide area operation and console operator positions, and computer equipment is used for interface between each of these equipment items. A standard should exist to describe any given specific instance of such a general land mobile radio system. This document will refer to such a specific instance of a general land mobile radio system as a "Land Mobile Radio system," to distinguish it from the entire universe of general land mobile radio systems. Specific Land Mobile Radio systems are referenced in the appendices for the instantiation of the security services described in this document.
TIA-102.AAAD, "Project 25 Digital Land Mobile Radio - Block Encryption Protocol"	The Project 25 standard covets all of the pans of a system (or public-safety Land Mobile Radio communications. These systems include portable radios for hand held operation, mobile radios for vehicular operation, base stations or fixed installations, and other fixed equipment for wide area operation and console operator positions, as well as computer equipment for data communications. The standard defines the means for this equipment to send and receive digital information, in the form of either voice or data (i.e. non-voice) messages.
TIA-102.AACA, "Project 25 Digital Radio Over-The-Air Rekeying (OTAR) Protocol"	This addendum specifies a method to transport Over The Air Rekeying (OTAR) Key Management Messages (KMMs) between a Key Management Facility (KMF) and an Mobile Radio (MR) that is independent of the physical and data transport layers. It defines optional key management procedures for Registration and Deregistration of the MR with the KMF. An Unable-To-Decrypt message has also been defined to respond to a message that was received and could not be decrypted.
TIA-102.AACB, "Project 25 Over-The-Air Rekeying (OTAR) Operational Description"	This document describes the basic keying concepts for protected radios, including those fundamental key management concepts related to Over-the-Air-Rekeying (OTAR). OTAR is an application layer process. Peer processes exist in the key management facility (KMF) and at the mobile radios. The KMF is responsible for providing OTAR functions for the set of mobile radios within its jurisdiction.

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

Standard Name	Standard Description
TIA-102.AACC-A, "Conformance Test for Project 25 Over-The-Air Rekeying (OTAR) Protocol"	This document provides a series of conformance tests for the Project 25 Over-The- Air-Rekeying (OTAR) Protocol, reference 1. These tests are intended to assure that the equipment conforms to the message formats specified in the OTAR Protocol document. This is a first step (necessary but not sufficient) for interoperability with other equipment conforming to the standard. These tests provide for the encryption of keys and the generation of the Message Authentication Code (MAC) that may be part of a Key Management Message (KMM). The tests generating KMM data messages, that may contain encrypted keys and/or a MAC, will not perform the outer layer encryption (the encryption of the data message with a traffic key). The output of these tests will generate a file containing plain text data message(s) suitable to be encrypted by the programs provided in the Conformance Test for the Project 25 DES Encryption Protocol, reference 2.
TIA-102AACD, "Project 25 Digital Land Mobile Radio Key Fill Device (KFD) Interface Protocol"	This document addresses the manual rekeying interface between a KFD and an MR only.
TIA-102.BAKA, "Project 25 KMF to KMF Interface"	This document covers, in detail, the Inter-KMF interface protocols, security mechanisms, and transport used to exchange encryption keys.
TIA-102.CABB, "Project 25 Interoperability Procedures Over-The-Air Rekeying (OTAR)"	The purpose of this document is to define procedures for testing the interoperability of Data, specifically, Over-The-Air-Rekeying (OTAR) commands between RF Sub-systems and Mobile Radio subscribers of different manufacturers, different models of the same manufacturer, and different firmware upgrades of the same model. This is the second of a series of documents, all of which discuss procedures for interoperability testing of TIA102 digital radio equipment. The contents of this document are confined to OTAR functions. As currently envisioned, other documents in the series will address capabilities of trunking, data transmissions, and networking. A prerequisite for interoperability testing is the requirement that the unit under test (UUT) meet the conditions of conformance and performance as designated in the TIA102 standards.
TIA-102.AACE-A, "Project 25 Digital Land Mobile Radio Link Layer Authentication"	The authentication service described in this document is applicable to FDMA and TDMA trunking systems using an FDMA trunking control channel. Authentication is a supplementary service for trunked radio systems. This document describes two forms of authentication: unit authentication and mutual authentication.