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

May 17, 2013

Via Electronic Filing (www.regulations.gov)

General Services Administration
Regulatory Secretariat (MVCB)
ATTN: Hada Flowers
1275 First Street, NE, 7th Floor, Washington, DC 20417

Re: Comments of the Telecommunications Industry Association to the General Services Administration on Improving Cybersecurity and Resilience through Acquisition (Notice-OERR-2013-01)

I. Introduction and Statement of Interest

The Telecommunications Industry Association ("TIA"), representing approximately 500 information and communications technology ("ICT") manufacturers, vendors, and suppliers, hereby submits comment on the General Services Administration's ("GSA") Joint Working Group on Improving Cybersecurity and Resilience through Acquisition Request for Information ("RFI") to inform its recommendations on increasing cybersecurity and resilience through Federal acquisition.[1] In accordance with Section 8(e) of Executive Order 13636, GSA must work jointly with the Department of Defense ("DOD") and in consultation with the Department of Homeland Security ("DHS") and the Federal Acquisition Regulation Council, make recommendations on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration and address what steps can be taken to harmonize, and make consistent, existing procurement

[1] *See* GSA, *Joint Working Group on Improving Cybersecurity and Resilience through Acquisition*, Request for information, 78 Fed. Reg. 27966- 27968 (May 13, 2013) ("RFI").

requirements related to cybersecurity.[2] These recommendations must be communicated to the President by June 12, 2013.

TIA appreciates the Administration's efforts to improve cybersecurity in Federal procurement. Generally, we urge that GSA proceed in its development of recommendations to the President 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 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 the EO and the related Presidential Policy Directive.[3] 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")[4] and the Federal Communications

---

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

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

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

Commission's ("FCC") Communications Security, Reliability and Interoperability Council ("CSRIC").[5] TIA also actively convenes its members to address issues related to the EO and PPD-21 in its Cybersecurity Working Group, and has recently released cybersecurity policy recommendations for critical infrastructure and the global supply chain[6] that have shaped our views below and in related filings with the National Institute of Standards and Technology ("NIST") on its planned Cybersecurity Framework[7] and the Department of Commerce on incentives to adopt improved cybersecurity polices.[8]

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.[9]

---

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

6 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).

7 http://www.tiaonline.org/sites/default/files/pages/TIA_Comments_NIST_Cybersecurity_Framework_040813.pdf

8 http://www.tiaonline.org/sites/default/files/pages/TIA-Comments-NIST-NTIA-Cybersecurity-Framework-Incentives-042913.pdf

9 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*

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.[10] 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 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 machine-to-machine ("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.[11]

---

http://www.tiaonline.org/standards_/about/documents/STAR_2012_Web.pdf ("TIA Standards Report"). TIA standards are available from IHS, Inc. *See* http://www.ihs.com/.

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

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

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

II. TIA Responses to Questions Posed in the GSA RFI

FEASIBILITY AND FEDERAL ACQUISITION:

2. How can the federal acquisition system, given its inherent constraints and the current fiscal realities, best use incentives to increase cybersecurity amongst federal contractors and suppliers at all tiers? How can this be accomplished while minimizing barriers to entry to the federal market?

We submit the following suggestions on ways to encourage federal contractors and suppliers at all tiers to increase cybersecurity while minimizing barriers to entry to the federal market:

Maintain the flexibility and the ability to innovate. When examining ways to incentivize federal contractors and suppliers generally to improve cybersecurity, the danger inherently exists to overgeneralize. TIA believes that an utmost concern for GSA in forming their recommendations to the President should be to respect the need for specific sectors to innovate and to address specific threats. By ensuring that this key principle is protected, the federal government would see more innovative products available to them at less cost. We believe this key concept includes technology neutrality – that the government set objectives in its procurement policies, but avoid in all cases possible the dictating of how a company that is involved in a procurement meets that objective. Not only does this promote innovation, but it prevents favoritism of one solution or company over others and in this way enhances competition.

"Critical infrastructure," was identified by DHS pursuant to Presidential Policy Directive #7 in 2003.[12] Under the EO, not later than July 12, 2013, the Secretary of Homeland Security must 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, which accompanied the release of the EO. Per the EO, DHS is the SSA

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

for communications. The EO, however, prohibits, the Secretary from identifying "any commercial information technology products or consumer information technology services" under this process. We note our support for 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, and believe that it illustrates the Administration's appreciation of this need. We urge GSA, in fulfilling its responsibilities surrounding the identification of critical infrastructure, not to stifle the ability of the manufacturers of the ICT equipment that enables each critical infrastructure sector to innovate, and instead to rely on each sector member to determine their needs through the ICT they comprise their service of. In short, GSA should ensure that the necessary flexibility and technology neutrality exists for effective cybersecurity-related procurements across sectors.

Recognizing the necessity of international approaches and standards. TIA urges GSA to ensure that their recommendations to the President reflect 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. Consistent with this theme, we urge the recognition 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. ICT products are often designed and built in different locations using globally-sourced components, making it very difficult to classify specific products as U.S. or non-U.S. products. Moreover, to control costs and manage supply chain risk, manufacturers need flexibility to change component suppliers for a particular product at any time. Aside from the complexity in defining the nationality of a particular product, ICT companies conduct different functions (manufacturing, R&D and services) across facilities in multiple different countries, often making it difficult to classify companies as U.S. or non-U.S. companies. To stay competitive, ICT companies need to continue to use a distributed approach to their technology development and manufacturing. ICT believe that an increasingly trusted global Internet and infrastructure goes hand-in-hand with these needs, the result fueling future growth globally, driving significant innovation and security in IT products and services, and resulting in billions of dollars in ICT R&D (which includes

R&D related to security) each year. This virtuous cycle of investment has spurred global standards for product assurance. As an example, TIA standards are used throughout the world across a number of technologies, as well as in other areas such as building codes.

Any approach taken by GSA should involve international cooperation and heavy engagement with the private sector, and should not include language that might put the government in a position to determine the future design and development of technology. TIA 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 federal activity pursuant to the EO 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 (please see below for our response to question 34), we believe that the U.S. should be a leader is this area.

Recognizing that the ICT industry is global, standards-based, interoperable, and that security needs are driven by innovation, and the build-once-sell-globally innovation and business model, TIA believes that the Executive Order seeks to ensure that the activities taken pursuant to it provide guidance that is 'technology neutral' – meaning that it doesn't get the government into the design, development, or manufacture of commercial ICT products, and doesn't pick winners and losers. This same sentiment is expressed in the leading drafts of U.S. legislation. To do otherwise would undermine the very innovation and security we need to promote security, and give other governments license to interfere with the core innovation engine of the ICT sector, impose country specific requirements, and pull apart the very innovation, interoperability, and global standards that are needed to drive security and innovation into the global network. Any country specific requirement would also undermine the Common Criteria, a global IT product evaluation methodology that undergirds security and innovation.

Based on the above, 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.

Fair assessments of trust with an impartial process for addressing concerns. For companies which contract with and vend to the federal government, attaining and maintaining the proper level of trust is of the upmost importance. We urge that any recommendations on improving cybersecurity reinforce the need for reasonable assessments along with a fair opportunity for concerns to be addressed by the contractor or vendor at issue.

Maintaining parity with Federal Information Security Management Act implementation. TIA supports efforts to improve and harmonize cybersecurity programs across government agencies. In doing so, TIA has urged policymakers to focus on the security practices of agencies and their personnel – people and processes – while avoiding ICT security requirements that could prove disruptive to the ICT supply chain. Consistent with our views that economic barriers for owners and operators of critical infrastructure is a crucial step in securing cyberspace,[13] we urge GSA to ensure that any improvements to security and privacy requirements that it places on contractors and vendors in the acquisition process is not inconsistent with FISMA implementation requirements on agencies,[14] and with widely used international standards and best practices. Consistency with existing commercial best practices and standards, as well as across the federal government, will encourage the broadest availability of products and services.

---

[13] TIA Cybersecurity Whitepaper at 5-6.

[14] Federal Information Security Management Act ("FISMA"), Public Law 107-347; Office of Management and Budget (OMB) Circular A-130.

This would also be consistent with the Clinger-Cohen Act, which strongly encourages the use of commercial-off-the-shelf technology.[15]

Providing credit-based or tax-based incentives. We have previously noted that incentives to improve cybersecurity can include tax credits for such investments, and believe that these incentives could also be effected through the federal acquisition process. While further consultation would be needed from a variety of stakeholders, we support the GSA recommending credit-based or tax-based incentives to the President as ways to improve cybersecurity in procurements.

Cybersecurity expertise as part of the acquisition process, and end-user education. A large challenge for reform in the acquisition process will be to ensure that cybersecurity concerns are fully appreciated and understood throughout that process. 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.[16]

3. What are the implications of imposing a set of cybersecurity baseline standards and implementing an associated accreditation program?

TIA appreciates the need to ensure the integrity of products and services procured by the federal government, but urges GSA to avoid creating any new regimes of baseline standards or associated accreditation programs. We believe that efforts to improve cybersecurity, including in

---

[15] *See* Clinger-Cohen Act (also known as "Information Technology Management Reform Act of 1996") (Pub. L. 104-106, Division E).

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

federal procurement, should leverage existing standardization and related accreditation programs in all cases possible. The communications sector is far ahead of others in efforts to improve the resilience of our Nation's critical infrastructure. Numerous 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, which TIA has discussed in more detail in related filings to NIST and DOC.[17] Government procurement processes use some of these standards and include companies attesting and/or demonstrating compliance with these standards, including:

- **the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408, known as the "Common Criteria")**, and the companion Common Methodology for Information Technology Security Evaluation ("CEM");[18]
- **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;[19]
- **the Open Group Trusted Technology Forum's ("OTTF") global supply chain integrity program and framework** that provides buyers of IT products with a choice of accredited technology partners and vendors;[20] and
- **the Software Assurance Forum for Excellence in Code ("SAFECode")**, guidance in information and communications technology products and services through the advancement of effective software assurance methods.[21]
- **SAE International AS5553 Standard - Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition.**[22]

---

17 *See* TIA NIST Cybersecurity Filing at ; *see also* TIA NIST-NTIA Cybersecurity Incentives Filing at .

18 *See* http://www.commoncriteriaportal.org/cc/.

19 *See* http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42509.

20 *See* http://www.opengroup.org/ogttf/.

21 *See* http://www.safecode.org/index.php.

22 *See* http://standards.sae.org/as5553/

- **TIA-942-A (Telecommunications Infrastructure Standard for Data Centers)**, which presents an infrastructure topology for accessing and connecting the respective elements in the various cabling system configurations currently found in the data center environment. In order to determine the performance requirements of a generic cabling system, various telecommunications services and applications were considered. In addition, this document addresses the floor layout related to achieving the proper balance between security, rack density, and manageability. TIA-942-A is utilized in over 70% of standardized data centers.

We emphasize to GSA that the creation of a new conformity assessment regime that is added on top of and ignores existing efforts will add cost to participating in procurements, and would disincentivize innovation in related products generally as a result and, more acutely, reduce the reasons for companies to participate in procurements. We urge GSA to take the approach used currently to verify some of the very standards listed above which include certifications of product conformance developed in association with the standard. Finally, as we also describe elsewhere in this filing, any US-centric standard would ignore 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. Going down the ill-advised path of creating a new standards and associated conformity assessment regime in lieu of existing successful efforts would in this way place US-based companies attempting to do business overseas in a compromised position.[23]

4. How can cybersecurity be improved using standards in acquisition planning and contract administration?

TIA believes that standards organizations that develop international standards should serve as a cornerstone in critical infrastructure cybersecurity federal procurement and conformity assessment, as they do now in many instances. The existing process utilized in the development of voluntary, industry-led and consensus-based standards allows for fluid, responsive, and rapid

[23] Unfortunately, there are other parts of the globe where "foreign" input is disregarded, and the standardization system is effectively used as a way to give preference to parties physically located within a country. We believe that the United States government is in alignment with other standardization stakeholders that such policies stifle innovation and investment.

improvements to these crucial standards. Standard developers and related organizations are already active in developing cybersecurity standards and conformity assessment, and should continue to play a key role. As we have described in filings to NIST and DOC as well as elsewhere in this response, a number of international standards cover cybersecurity and cybersecurity conformity assessment across the ICT landscape, such as SAFEcode, SAE-5553, the Trusted Technology Forum, and the Common Criteria. Others are being developed, such as the security assurance methodology for mobile networks now addressed by 3GPP Systems Aspects (SA) 3. These form part of the landscape of global standards and best practices that will continue to evolve in the future. Consequently any changes to acquisition planning and contract administration by GSA or other federal actors should (1) utilize the effective and dynamic work already ongoing and (2) neither stifle innovation nor constrain such industry-driven evolution by any prescriptive regulation on conformity assessments.

5. **What are the greatest challenges in developing a cross-sector standards-based approach cybersecurity risk analysis and mitigation process for the federal acquisition system?**

Our discussing in the above questions also addresses these issues, but from the approach of how a standards-based approach and other incentives can be used to improve cybersecurity risk analysis and mitigation processes for the federal acquisition system. Building on those recommendations above, we note that there are numerous challenges in developing a cross-sector standards-based approach cybersecurity risk analysis and mitigation process for the federal acquisition system, including but not limited to:

Fully leveraging public-private partnerships. TIA believes that efforts to improve cybersecurity risk analysis and mitigation processes, including in federal procurement policies, should leverage public-private partnerships as an effective tool for collaboration on addressing current and emerging threats. We consider the public-private partnership model to be a key element of a cross-sector standards-based approach. Public-private partnerships have been recognized as the basis for the cyber defense of critical infrastructure and cybersecurity policy

for the last decade.[24] 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 GSA and other United States government agencies leverage and augment existing public-private partnerships. TIA members believe that any steps taken that would reduce the effectiveness of the public-private partnership model would have a negative impact on the security of critical infrastructure. We note that the National Infrastructure Protection Plan ("NIPP"), which has formalized the public-private partnerships in the 18 critical infrastructure sectors with Sector Specific Plans and Sector Coordinating Councils ("SCCs") describes the benefits of the public-private partnership as follows:

> The multidimensional public-private sector partnership is the key to success in this inherently complex mission area. *** [It] has facilitated closer cooperation and a trusted relationship in and across the 18 CIKR sectors. *** Integrating multi-jurisdictional and multi-sector authorities, capabilities, and resources in a unified but flexible approach that can also be tailored to specific sector and regional risk landscapes and operating environments is the path to successfully enhancing our Nation's CIKR protection.
>
> Implementation of the NIPP is coordinated among CIKR partners to ensure that it does not result in the creation of duplicative or costly risk management requirements that offer little enhancement of CIKR protection. *** The NIPP provides the framework for the unprecedented cooperation that is needed to develop, implement, and maintain a coordinated national effort to bring together government at all levels, the private sector, nongovernmental organizations, and international partners.[25]

We note our belief 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

---

[24] 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.

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

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 inform, on a rolling basis, federal procurement policies at issue, 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 serve as the foundation for moving forward with critical infrastructure protection, including recommendations made by GSA to the President on ways to improve federal procurement.

Liability. When there is a risk of serious liability, there is also an inherent disincentive to take risk and enter a market. The assurance of liability protection for organizations that act in good faith as part of their contracting with the Federal government will serve as a crucial enabler of this incentive (for both industry and government).

Insufficient cybersecurity research and development. Initially, we note our understanding of the effect that sequestration may have on federally-funded programs and procurements. Nonetheless, 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.[26] The resulting effects on the U.S. ICT sector of a less competitive ICT research ecosystem are tangible, and the results touch the Federal government as well as the private sector. As far back as 2009, the National Academy of Sciences stated that "[t]he nation risks

---

[26] 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.

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."[27] 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. This trend is a significant challenge in developing a cross-sector standards-based approach cybersecurity risk analysis and mitigation process for the federal acquisition system. TIA believes that Federal funding for cybersecurity research and development should be prioritized, and should coordinate research activities amongst contributing agencies, incorporating industry input.

6. What is the appropriate balance between the effectiveness and feasibility of implementing baseline security requirements for all businesses?

Please see TIA's response to question 2, specifically our discussion of maintaining the ability to innovate and reliance upon industry-led voluntary and consensus-based standards, and the ways that these and other approaches described in question 2 appropriately balance between the effectiveness and feasibility of implementing baseline security requirements for all sectors.

7. How can the government increase cybersecurity in federal acquisitions while minimizing barriers to entry?

Please see TIA's response to question 2, specifically our discussion of the necessity of international approaches and standards, as well as our discussion about the benefits of global standards generally below in question 33.

8. Are there specific categories of acquisitions to which federal cybersecurity standards should (or should not) apply?

TIA believes that it is a logical approach for acquisitions to which federal cybersecurity standards would apply to be classified, and that one approach may be to use the level of cyber threat, determined by such factors as potential danger and possible bearings on Federal systems.

---

[27] 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.

We urge GSA that in some ways, less can be more when taking this approach. By finding the appropriate balance of commonality and using bright-line and rational differentiation, we believe that GSA can avoid creating an overly-complicated myriad of categories and varied requirements that would keep some ICT manufacturers and vendors away. A good first step for GSA is to ensure that they build on existing federal procurement guidelines to avoid duplicative efforts that may not incorporate lessons learned from past processes used. Finally, we urge that extra care be taken to ensure that commonality across the federal government be a priority.

10. How can the Federal government change its acquisition practices to ensure the risk owner (typically the end user) makes the critical decisions about that risk throughout the acquisition lifecycle?

In general TIA supports providing federal Chief Information Officers ("CIOs") with increased authority over IT expenditures. We believe that this is consistent Clinger-Cohen Act.[28] However, concentrating budget authority with department level CIOs can also limit innovation and needed flexibility at operational level where much of the IT purchasing occurs, and can slow the acquisition process. Agency CIOs should be trained to develop enhanced acquisition skills that also encourage the consideration of necessary cybersecurity concerns. Finally, we again note that consistency across agencies is crucial to support effective implementation.

12. How would you recommend the government evaluate the risk from companies, products, or services that do not comply with cybersecurity standards?

We believe that federal agencies should fairly and carefully evaluate companies, products, and services which they believe not to be in compliance with cybersecurity standards. If the federal government determines an issue with an private organization, we urge that reasonable assessments be utilized along with a fair opportunity for concerns to be addressed by the contractor or vendor at issue. Part of this process should include an agency-internal examination of processes and activities to ensure that all parties to the transaction that procured the service or product acted appropriately.

---

[28] *See* Clinger-Cohen Act at.

COMMERCIAL PRACTICES:

13. To what extent do any commonly used commercial standards fulfill federal requirements for your sector?

Commercial standards – which we wish to note we interpret in this case to mean industry-led, voluntary, open, and consensus-based standards – are sometimes used to fulfill federal requirements in the ICT sector. For common examples, we refer you to the non-exclusive list above in question 3 (noting the Common Criteria, the ISO/IEC 27000-series, the OTTF, SAFECode, SAE-5553, and TIA-942-A). As an example, the Common Criteria is required for sale into National Security Systems, and that system is run by the National Information Assurance Partnership (NSA/NIST).[29] As a global standard for product assurance for national security systems, Common Criteria allows the ICT industry to build-once and sell-globally, and allows for evaluations by non-governmental independent labs, and mutual recognition by CCRA countries, avoiding disparate and conflicting country-specific requirements that would undermine interoperability and security of the network. Further, the use of independent labs (accredited by the CCRA schemes) helps ensure the protection of the core intellectual property and innovation of IT companies. Per the National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, the Common Criteria is required for commercial products used in national security telecommunications and information systems, and GSA should ensure that it does nothing to undermine the CC (NSA/NS) methodology for product security and evaluation. In addition, those same products carrying the CC evaluation may be used in many civil Federal networks. We also emphasize however that any non-national security commercial off-the-shelf ("COTS") procurement requirements should allow industry flexibility through self-certification and global acceptance based on international standards.

[29] *See* http://www.niap-ccevs.org/.

We also note our longstanding position that when an industry-led, voluntary, open, and consensus-based standard is included in *regulations*, the use should be as a safe harbor – *not* a requirement – when possible in order to provide the greatest amount of flexibility for innovation and simultaneous compliance. However, it is also vital that the multiple standards and approaches be allowed and encouraged in order not to limit innovation or stifle technological advances.

14. Is there a widely accepted risk analysis framework that is used within your sector that the federal acquisition community could adapt to help determine which acquisitions should include the requirement to apply cybersecurity standards?

While these are non-exclusive examples and are discussed in much further detail above, the Common Criteria and the ISO/IEC 27000-series are prominent examples of widely accepted risk analysis frameworks that are used within the IT sector that the federal acquisition community has already adapted to help determine which acquisitions for national security systems should include the requirement to apply cybersecurity standards.

15. Describe your organization's policies and procedures for governing cybersecurity risk. How does senior management communicate and oversee these policies and procedures? How has this affected your organization's procurement activities?

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.[30] Other important factors include those noted in the 20 Critical Controls,[31]

---

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

31 *See* http://www.sans.org/critical-security-controls/.

all of which were recently determined by the FCC's CSRIC to be applicable to the enterprise communications networks.[32]

16. Does your organization use "preferred" or "authorized" suppliers or resellers to address cybersecurity risk? How are the suppliers identified and utilized?

ICT manufacturers and vendors work hard to secure preferred or authorized statuses with federal agencies. Industry-led standards naturally address this need (for example, please see our description and link to more information on the OTTF's global supply chain integrity program and framework above in question 3). In addition to collaboration in open, voluntary, and consensus-based for a, individual companies have in place their own processes to ensure their suppliers are trusted due to competitive market demands. Authorized manufacturers and suppliers are already working to make sure networks are as resilient and reliable as possible, and have incentives to do so, usually on a contractual basis, in order to remain competitive in the market.

[32] *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.

HARMONIZATION:

32. What cybersecurity requirements that affect procurement in the United States (e.g., local, state, federal, and other) has your organization encountered? What are the conflicts in these requirements, if any? How can any such conflicts best be harmonized or de-conflicted?

We defer to individual companies to note specific issues that may have arisen for them in specific procurements domestically. However, harmonization of procurement policies across government agencies is a very high priority for TIA. We refer GSA to our responses above in question 5, particularly related to fully leveraging public-private partnerships, which serve as invaluable venues for public-private (and, importantly, public-public) information sharing and collaboration.

33. What role, in your organization's view, should national/international standards organizations play in cybersecurity in federal acquisitions?

Generally, voluntary, open, and consensus-based standards are a powerful tool for organizations of all sizes, private and governmental, and support innovation as well as increased productivity. Specifically, these standards:

- **Promote efficiency and interoperability:**
  - Enhance industry collaboration to solve market-driven demands and customer needs.
- **Enable access to new technologies and markets:**
  - Help diffuse innovative solutions across the industry while maintaining respect for intellectual property rights and supporting incentives for companies to further invest in related R&D.[33]
  - Create opportunities for further competition among differentiated implementations and products, which provides stimulus for more innovation and choice for customers and users.

[33] *See* TIA, *Intellectual Property Rights Standing Committee Paper on Open Standards* (Jun. 20, 2008), *available at* http://www.tiaonline.org/standards/about/documents/TIA-IPR_20080620-003_TIA_OPEN_STANDARDS.pdf.

In no sector more than ICT must standards constantly be updated to remain relevant. To remain pertinent and useful, and to take into account the latest technical solutions to aide in moving the industry forward, TIA standards are continuously developed and reviewed. These standards frequently compete with other standards in an extremely vibrant international environment, facilitating market-driven growth, industry competitiveness and choice.[34] In some cases, however, products implementing a standard may not automatically solve a technology challenge. Adherence to a standard may not ensure that competing products will actually interoperate. Further industry collaboration often may be necessary (such as conformance and interoperability testing) in order to accomplish specific objectives.

For governmental entities, the ability to partake in voluntary consensus standard development has many benefits and is consistent with goals of the U.S. Government as reflected in the National Technology Transfer and Advancement Act and OMB Circular A-119.[35] TIA believes that the OMB Circular has been very effective, and supports its recognition of the value of "voluntary consensus standards." This term is defined broadly to include standards from ANSI-accredited SDOs and also a wide range of consortia, further evidencing the U.S. Government's recognition of the value of having competition and diversity among SDOs.

Furthermore, because standardization is a form of economic self-regulation, it can relieve the government of the responsibility for developing detailed technical specifications while ensuring that voluntary consensus standards serve the public interest, saving resources that can be used to serve the public interest in other ways. Standards may be used to define an acceptable level of performance, and through participation in the process, a governmental entity can work to ensure

---

[34] For example, the choice with respect to US wireless technology between the CDMA-train standards developed by TIA and 3GPP2, and the GSM-train standards developed by ETSI and 3GPP (including ATIS, the US-based 3GPP-sponsoring organization).

[35] NIST has a coordinating function with the U.S. Government under the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113), which is further implemented through OMB Circular A-119. *See* OMB Circular A-119 Revised, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities (rev. Feb. 10, 1998) (OMB Circular A-119) *available at* http://www.whitehouse.gov/omb/rewrite/circulars/a119/a119.html.

that an adequate level of service is offered to the public in a particular area. In some limited instances, the government has made standards legally binding to assure a minimum level of public safety through safe harbors.[36] In addition, standards may also be used by government entities as valuable sources of scientific and technical information, allowing for agencies to use standards as a resource for advanced technical information without first-hand independent knowledge of research in the area.

As we have described above in question 2, TIA urges GSA to ensure that their recommendations to the President reflect 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. We urge the recognition 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 by the Federal government 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 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. Our concerns in this area are described in more detail above in question 2. GSA should take great care to avoid enacting cybersecurity policies that would restrict trade in

---

[36] Section 107(a)(2) of CALEA contains a safe harbor provision, stating that "[a] telecommunications carrier shall be found to be in compliance with the assistance capability requirements under section 103, and a manufacturer of telecommunications transmission or switching equipment or a provider of telecommunications support services shall be found to be in compliance with section 106 if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the Commission under subsection (b), to meet the requirements of section 103." 47 U.S.C. § 1006(a)(2). Subcommittee TR-45.2 of TIA, along with Committee T1 of ATIS, developed interim standard J-STD-025 to serve as a "safe harbor" for wireline, cellular, and broadband PCS carriers and manufacturers under section 107(a) of CALEA. The standard defines services and features required by wireline, cellular, and broadband PCS carriers to support lawfully authorized electronic surveillance, and specifies interfaces necessary to deliver intercepted communications and call-identifying information to a law enforcement agency. *See* TIA, Communications Assistance for Law Enforcement Act (CALEA), *available at* http://www.tiaonline.org/standards/technology/calea/ (last visited February 22, 2011).

telecommunications equipment imported to, or exported from, other countries that are part of the global trading system.

34. What cybersecurity requirements that affect your organization's procurement activities outside of the United States (e.g., local, state, national, and other) has your organization encountered? What are the conflicts in these requirements, if any? How can any such conflicts best be harmonized or de-conflicted with current or new requirements in the United States?

We decline to call out any specific examples and defer to our individual members to note specific issues that may have arisen for them in specific procurements internationally. However, harmonization of procurement policies across borders is a very high priority for TIA and we offer the following recommendations for the GSA in their assessment for the President:

- Enhance international outreach and cooperation by the U.S. Government is critical to developing common approaches to cybersecurity as other governments formulate domestic cybersecurity policies affecting government procurement.
- Encourage governments to work in partnership with industry as they development cybersecurity policies and related government procurement policies.
- Emphasize the use of relevant internationally developed standards to the extent feasible in the development of technical regulations affecting government procurement.

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

III. Conclusion

We urge the consideration of the above views on the part of the ICT manufacturer, supplier, and vendor community, and we look forward to future engagement with GSA, DOD, and other Federal agencies as policies are formulated and implemented pursuant to the Executive Order.

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
1320 North Courthouse Road
Suite 200
Arlington VA 22201

May 17, 2013