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

April 28, 2014

General Services Administration
Regulatory Secretariat Division (MVCB)
ATTN: Ms. Flowers
1800 F Street NW, 2nd Floor
Washington, DC 20405

Comments of the Telecommunications Industry Association to the General Services Administration on Implementing the Final Report of the Joint Working Group on Improving Cybersecurity and Resilience through Acquisition (Notice-OMA-2014-01)

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
Brian Scarpelli
Director, Government Affairs
1320 North Courthouse Road
Suite 200
Arlington VA 22201

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

Table of Contents

I. INTRODUCTION AND STATEMENT OF INTEREST 1

II. TIA VIEWS ON IMPLEMENTING THE JOINT WORKING GROUP'S REPORT ON IMPROVING CYBERSECURITY AND RESILIENCE THROUGH ACQUISITION 3

A. GSA should provide clarity regarding the scope of the recommendations and intended changes. 3

B. Efforts to implement the Report's recommendations should ensure flexibility and the ability to innovate. 3

C. Efforts to implement the Report's recommendations should recognize the necessity of international approaches and standards. 4

D. DoD and GSA should use caution in imposing a set of cybersecurity baseline standards. 5

E. Cybersecurity expertise as part of the acquisition process, and end-user education. 7

F. TIA supports the Report's recommendation to develop common cybersecurity definitions for Federal acquisitions. 8

G. Federal acquisition risk management strategies should rely on voluntary, open, and consensus-based standards where possible. 9

H. TIA views on the Report's recommendation to purchase from original equipment or component manufacturers, their authorized resellers, or other "trusted" sources. 11

I. TIA supports efforts to increase government accountability 12

III. CONCLUSION 13

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

April 28, 2014

Via Electronic Filing (www.regulations.gov)

General Services Administration
Regulatory Secretariat Division (MVCB)
ATTN: Ms. Flowers
1800 F Street NW, 2nd Floor
Washington, DC 20405

Re: Comments of the Telecommunications Industry Association to the General Services Administration on Implementing the Final Report of the Joint Working Group on Improving Cybersecurity and Resilience through Acquisition (Notice-OMA-2014-01)

I. INTRODUCTION AND STATEMENT OF INTEREST

The Telecommunications Industry Association ("TIA"), representing hundreds of information and communications technology ("ICT") manufacturers, vendors, and suppliers, hereby submits comment on the General Services Administration's ("GSA") in response to its Request for Information ("RFI") on implementation of the Final Report of the Joint Working Group on Improving Cybersecurity and Resilience through Acquisition which makes six recommendations to improve cybersecurity and resilience in Federal acquisitions[1] in accordance with Section 8(e) of Executive Order 13636.[2]

---

[1] *See* GSA, *Joint Working Group on Improving Cybersecurity and Resilience through Acquisition*, Notice With A Request For Comments, 79 FR 14042 (Mar. 12, 2014) ("RFI"); see also DoD and GSA, *Improving Cybersecurity Resiliency Through Acquisition: Final Report of the Department of Defense and General Services Administration* (rel. Nov. 2013) ("Report").

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

TIA appreciates the Administration's efforts to improve cybersecurity in Federal procurement. Generally, we urge that implementers of the Report be guided by the following principles:

- that successful efforts to improve cybersecurity will leverage public-private partnerships to effectively collaborate on addressing current and emerging threats;
- that the U.S. government should enable and stimulate greater cyber threat information sharing between the public and private sector;
- that policymakers and regulators should ensure that they address economic barriers for owners and operators of critical infrastructure in efforts to secure cyberspace;
- 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.

TIA represents approximately 400 ICT manufacturer, vendor, and supplier companies in government affairs and 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.[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 and Information Technology Coordinating Councils and the Federal Communications Commission's Communications Security, Reliability and Interoperability Council ("CSRIC"), among other successful public-private partnerships. TIA also actively convenes its members to address issues related to the EO and PPD-21 in its Cybersecurity Working Group.

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

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

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.[4]

II. TIA VIEWS ON IMPLEMENTING THE JOINT WORKING GROUP'S REPORT ON IMPROVING CYBERSECURITY AND RESILIENCE THROUGH ACQUISITION

TIA appreciates the efforts of the Joint Working Group to fulfill the requirements of Section 8(e) of Executive Order 13636 which sought recommendations from DoD and GSA on "the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration."[5] Consistent with our previous views, we submit the following suggestions on ways to implement the recommendations in the Report that will encourage federal contractors and suppliers at all tiers to increase cybersecurity while minimizing barriers to entry to the federal market.

A. GSA should provide clarity regarding the scope of the recommendations and intended changes.

Initially, TIA notes that the Report does not provide sufficient details as to whether the implementation of the Report will impact all Federal acquisitions, or if some types of acquisitions will be exempt. We urge for GSA to address this to resolve related uncertainty the manufacturer and supplier community.

B. Efforts to implement the Report's recommendations should ensure 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 in planning the implementation of the Report's recommendations should be to respect the need for specific sectors to innovate and to address specific threats. We have previously noted that 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 concept includes

---

[4] 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 (2013), *available at* https://www.tiaonline.org/sites/default/files/pages/STAR2013withLinks.pdf.

[5] *See* EO at Section 8(e).

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. We have urged DoD and GSA not to stifle the ability of the manufacturers of the ICT equipment that enables suppliers of systems across the Federal government to innovate, and instead to rely on specific stakeholders to determine their needs through the ICT they comprise their systems of. In short, GSA should ensure that the necessary flexibility and technology neutrality exists for effective cybersecurity-related procurements across sectors.

C. Efforts to implement the Report's recommendations should recognize the necessity of international approaches and standards.

TIA has previously urged DoD and GSA to maintain 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. The Report appreciates the role of the global nature of the ICT industry which requires a global approach to address cybersecurity concerns, and we again emphasize 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. The Report includes discussion of this topic,[6] which TIA commends.

To stay competitive, ICT companies need to continue to use a distributed approach to their technology development and 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.

Any approach taken by DoD and GSA in implementing the Report's recommendations 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

[6] *See*, *e.g.*, Report at 11.

design and development of technology. TIA believes that the United States should work with other stakeholders to establish international security standards in order to prevent hobbling United States industry with United States-only standards. We remain concerned about the impact on both 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, we believe that the GSA should be a leader is this area.

Recognizing that the ICT industry is global, standards-based, interoperable; 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 or development commercial ICT products. 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 important already-relied upon standards such as the Common Criteria, a widely-used global ICT product evaluation methodology in this space.

D. DoD and GSA should use caution in imposing a set of cybersecurity baseline standards.

The Report states that:

> Often, cybersecurity requirements are expressed in terms of compliance with broadly stated standards and are included in a section of the contract that is not part of the technical description of the product or service the government seeks to acquire. This practice leaves too much ambiguity as to which cybersecurity measures are actually required in the delivered item. This recommendation envisions requirements for baseline cybersecurity requirements for contractor operations as well as products or services delivered to the governments.[7]

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

[7] Report at 14.

associated accreditation programs. We believe that efforts to improve cybersecurity, including in federal procurement, should leverage existing standardization and related accreditation programs in all cases possible. As TIA described in its initial comments to GSA and DoD to inform the Report's recommendations, 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.[8]

Previously, in comments to inform the Report, TIA has emphasized that cybersecurity requirements should be outcome-driven, not focused on the process by which a contractor may innovate to get to that outcome. The Report's direction to move away from relying on security standards may lend to 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 which would disincentivize innovation in related products generally as a result and, more acutely, reduce the reasons for companies to participate in procurements. We believe that the Federal government should take the approach used currently to verify some of these same standards which include certifications of product conformance developed in association with the standard. However, it may be helpful for agencies to ensure requirements on compliance with these standards in the technical description portion of the contract.

This concept is also important because any US-centric baseline standard created pursuant to the Report, whether intended or in effect, 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 will place US-based companies attempting to do business overseas in a compromised position.[9]

---

[8] *See* TIA Comments to the National Institute of Standards and Technology on Developing a Framework To Improve Critical Infrastructure Cybersecurity (Docket Number 130208119–3119–01) at 14-19; *see also* TIA Comments to the National Institute of Standards and Technology and National Telecommunications and Information Administration on Incentives To Adopt Improved Cybersecurity Practices (Docket Number 130206115–3115–01)NIST-NTIA Cybersecurity Incentives Filing at 15-20.

[9] 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.

E. Cybersecurity expertise as part of the acquisition process, and end-user education.

TIA has long noted that a large challenge for reform in the acquisition process will be to ensure that cybersecurity concerns are fully appreciated and understood throughout that process, and that 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." In our previous comments to GSA and DoD to inform the Report, we noted our support for 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.[10]

TIA notes its supports providing federal Chief Information Officers ("CIOs") with increased authority over IT expenditures. We believe that this is consistent Clinger-Cohen Act.[11] 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.

We commend the Report's inclusion of a recommendation to address cybersecurity in relevant training. However, this section appears to emphasize that "the government will require more from industry relative to cybersecurity in certain types of acquisition."[12] Indeed, industry has a role in increasing education on ways to improve resiliency to cyber-based vulnerabilities. However, the role of the Federal workforce training process is also very important. We strongly urge that the implementation of this recommendation reflect that reality.

---

10 *See* CSRIC Working Group 2A Report.

11 *See* Clinger-Cohen Act (Pub. L. 104-106, Division E).

12 Report at 14-15.

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

F. TIA supports the Report's recommendation to develop common cybersecurity definitions for Federal acquisitions.

The Report rightly includes a recommendation to ensure that there is a common understanding of key cybersecurity terms.[13] TIA agrees that this would have benefits across Federal agencies and the private sector. We particularly agree with the Report's statement that a good baseline for these definitions are consensus-based, international standards.[14] While the Report notes its intent to have this recommendation align, within the Federal government, with the DFARS effort on detection and avoidance of counterfeit electronic parts,[15] we also urge for alignment among other key efforts including the existing NIST Cybersecurity Framework and its future iterations.

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 removing economic barriers for stakeholders is a crucial step in securing cyberspace, we urge GSA to ensure that any changes to cybersecurity requirements that it places on contractors and vendors in the acquisition process is not inconsistent with FISMA implementation requirements on agencies,[16] 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. This would again be consistent with the Clinger-Cohen Act, which strongly encourages the use of commercial-off-the-shelf technology.[17]

---

13 Report at 15.

14 Report at 15.

15 Report at 15.

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

17 *See* Clinger-Cohen Act.

G. Federal acquisition risk management strategies should rely on voluntary, open, and consensus-based standards where possible.

TIA believes that standards organizations that develop international standards should serve as a cornerstone in Federal risk management. The existing process utilized in the development of voluntary, industry-led and consensus-based standards allows for fluid, responsive, and rapid improvements to these crucial standards, and is relied upon in the NIST Cybersecurity Framework, which the Report notes efforts per this recommendation should be harmonized with. Standard developers and related organizations are already active in developing cybersecurity standards useful in risk management. For example, the Common Criteria and the ISO/IEC 27000-series are prominent examples of widely accepted risk analysis frameworks that are used within the ICT 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. These and numerous others form part of the landscape of global standards and best practices that will continue to evolve in the future. This approach also allows for flexibility needed in an approach that would be applied across the Federal government. Consequently any new or changed risk management approach 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.

The approach of how a standards-based method 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 widely adaptable 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.[18] 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

[18] 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.

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. The recently-updated National Infrastructure Protection Plan ("NIPP 2013") describes the benefits of the public-private partnership as follows:

> The public-private partnership is central to maintaining critical infrastructure security and resilience. A well-functioning partnership depends on a set of attributes, including trust; a defined purpose for its activities; clearly articulated goals; measurable progress and outcomes to guide shared activities; leadership involvement; clear and frequent communication; and flexibility and adaptability. All levels of government and the private and nonprofit sectors bring unique expertise, capabilities, and core competencies to the national effort. Recognizing the value of different perspectives helps the partnership more distinctly understand challenges and solutions related to critical infrastructure security and resilience.[19]

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, improved cybersecurity resiliency in Federal procurements, including the National Coordination Center/Communications Information Sharing and Analysis Center, the National Cybersecurity and Communications Integration Center, the Partnership for Critical Infrastructure Security, the Control Systems Security Program, the Communications Coordinating Council, the IT Coordinating Council, the Network Security Information Exchange, the Cross-Sector Cyber Security Working Group, the FCC's CSRIC, and the National Security Telecommunications Advisory Committee. These and other public-private partnerships should serve as the foundation for moving forward with critical infrastructure protection, including implementing the recommendations of the Report.

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).

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 actions by GSA towards 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. We have previously detailed to

---

[19] NIPP 2013, Partnering for Critical Infrastructure Security and Resilience, 13 (2013) *available at* http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience.

the DoD our concerns related to this issues under its examination of changes to its rules on the resiliency of supply chains, which we urge implementers of the Report to review.[20]

H. TIA views on the Report's recommendation to purchase from original equipment or component manufacturers, their authorized resellers, or other "trusted" sources.

TIA supports the Report's recommendation to purchase from original equipment or component manufacturers, their authorized resellers, or other "trusted" sources, whenever available, in appropriate acquisitions.[21] ICT manufacturers and vendors work hard to secure preferred or authorized statuses with Federal agencies. Industry-led standards naturally address this need. In addition to collaboration in open, voluntary, and consensus-based efforts, 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.

TIA agrees with the Report that in some circumstances "limiting [procurement] eligibility to only [OEMs and their designated suppliers or resellers] for *all* acquisitions may not be compatible with acquisition rules, socioeconomic procurement preferences, or principles of open competition." For example, there may be circumstances where genuine ICT equipment replacements may not be produced by the OEM any longer, and the needed equipment is identified or marked by a source other than the part's legally authorized source. The Report recommends that:

> If the government chooses to use a reseller, distributor, wholesaler, or broker that is not in a trusted relationship with the OEM, then the government should obtain assurances of the company's ability to guarantee the security and integrity of the item being purchased. Such a trusted supplier compliance requirement is especially important when acquiring obsolete, refurbished, or otherwise out-of-production components and parts.[22]

---

[20] *See* TIA Comments to the Department of Defense's Defense Federal Acquisition Regulation Supplement: Requirements Relating to Supply Chain Risk (DFARS Case 2012-D050) (filed Jan. 20, 2014), *available at* http://www.tiaonline.org/sites/default/files/pages/TIA%20Comments%20-%20DoD%20DFARS%20Requirements%20Relating%20to%20Supply%20Chain%20Risk%20%28DFARS%20Case%202012-D050%29%20011714.pdf .

[21] *See* Report at 17.

[22] Report at 18.

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

TIA agrees that attaining such assurances have value, but do not fully address the recurring issue of procurement officials consciously choosing to purchase from untrusted sources based purely on the cost factor. TIA recommends that, for circumstances where the Federal government determines there is a compelling need to procure from outside of a trusted channel, the procurement official should be required to attain (in writing) permission to do so from a designated official within the agency, and this decision should be made publicly available. We believe that these steps are necessary in the procurement process to ensure that risk – as well as cost – factor into decisions to purchase from outside of trusted channels.

I. TIA supports efforts to increase government accountability

Lastly, TIA briefly notes that it supports the Report's recommendations to increase government transparency in the acquisition process, and stands ready to work with all Federal agencies to help implement this recommendation.

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 EO and the Report.

Respectfully submitted,

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

By: */s/ Brian Scarpelli*

Brian Scarpelli
Director, Government Affairs

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

April 28, 2014