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

Response of the Telecommunications Industry Association to the Department of Homeland Security's Solicitation Number RFI20140220, *Cyber Security Solutions for Small/Medium Sized Businesses*

April 4, 2014

Point of Contact:

Brian Scarpelli
Director, Government Affairs
Telecommunications Industry Association (TIA)
1320 North Courthouse Rd, Ste 200
Arlington, VA 22201
d: 703.907.7714
BScarpelli@tiaonline.org
tiaonline.org

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 4, 2014

Filed electronically via email (Joseph.Hatzipanagiot@hq.dhs.gov)

Joseph Hatzipanagiotis,
Contract Specialist
Department of Homeland Security
Office of the Chief Procurement Officer
Washington, DC 20528

Re: ***Cyber Security Solutions for Small/Medium Sized Businesses (Solicitation Number RFI20140220)***

I. Introduction and Statement of Interest

The Telecommunications Industry Association ("TIA") submits comments to the Department of Homeland Security ("DHS") in response to its request for information[1] ("RFI") on industry capacity to provide broadly scalable cyber security solutions at an affordable cost to Small and Medium Businesses ("SMBs") in support of adoption of the National Institute of Standards and Technology ("NIST")-developed Framework for Improving Critical Infrastructure Cybersecurity (the "NIST Cybersecurity Framework").[2]

TIA, serving both the role of an industry-consensus policy advocate as well as of an American National Standards Institute-accredited standards developer, represents hundreds of information and communication technology ("ICT") manufacturer, vendor, integrator, and supplier companies and organizations that are directly impacted by DHS' activities in this space. Numerous TIA members are companies producing ICT products and systems, creating information security-related technologies, and providing ICT services information systems, or

---

1 DHS, *Cyber Security Solutions for Small/Medium Sized Businesses,* Solicitation No. RFI20140220 (Feb. 20, 2014), *available at* https://www.fbo.gov/index?s=opportunity&mode=form&id=445897314f062c28648d6692baef9257&tab=core&_cview=0.

2 *See* NIST, *Framework for Improving Critical Infrastructure Cybersecurity v. 1.0* (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

components of information systems. These products and services innovatively serve many of the sectors directly impacted by the EO[3] and the related Presidential Policy Directive.[4] Representing our membership's commitments in this area, we hold membership and are actively engaged in key public-private efforts that contribute to secure information systems, including the Communications Sector Coordinating Council ("CSCC") and Information Technology Sector Coordinating Council ("ITSCC"), and the Federal Communications 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.[6]

II. TIA Input on DHS's Request for Information

a. *TIA has concern with DHS using FedBizOps.gov for RFIs.*

Initially, TIA notes its concern with the platform chosen by DHS for this RFI. Why was www.FedBizOps.gov, the single government point-of-entry for Federal government procurement opportunities over $25,000, chosen as the means for soliciting this comment, as opposed to the Federal Register? In addition, TIA is not aware of www.FedBizOps.gov being typically used for "market research."

Further, we note that DHS has consistently used the Federal Register and its online comment system at www.regulations.gov for requests for input, and that www.regulations.gov provides agencies with the capability to strip comments of confidential input which is appropriately marked. We urge for DHS to use consistent platforms and practices when soliciting input from stakeholders in a request for information.

---

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

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

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

6 For more on TIA's Cybersecurity Working Group, please visit https://www.tiaonline.org/policy/cybersecurity.

b. *Context and clarity on the purpose of this RFI, and what responses will be used to inform, is needed.*

TIA does not believe that the RFI adequately provides context for or clearly state the purpose of the RFI. We maintain that this context and clarity is a crucial threshold to public commenters in order to provide meaningful input.

The RFI states that DHS is seeking "information from industry on its capacity to provide broadly scalable cyber security solutions at an affordable cost to [SMBs] in support of adoption of the [NIST Cybersecurity Framework]." However, DHS further provides a rather large disclaimer which elaborates in detail on what this RFI is *not*, including that:

- The RFI is "issued solely for information and market research planning purposes, and does not constitute a solicitation or a promise to issue a solicitation."
- That "those who respond to this RFI should not anticipate feedback with regards to its submission; other than acknowledgment of receipt - ONLY IF a request for an acknowledgement is requested by the submitter."
- That the "RFI does not commit the Government to contract for any supply or service... [and that DHS] "is not seeking proposals at this time."

To allow for commenters to provide the most informed input, DHS should clearly define what such input would be used for. Furthermore, for TIA and its members who have long been heavily engaged with the drafting and finalization of the NIST Cybersecurity Framework as well as the shaping of programs to support the adoption of it, DHS provides no linkage to such existing programs. Most notably, the RFI does not once mention the DHS C³ Voluntary Program (described at its launch by Acting Under Secretary for the National Protection and Programs Directorate Suzanne Spaulding as a "public-private partnership designed to help align critical infrastructure owners and operators with existing resources that will assist their efforts to adopt the Cybersecurity Framework and manage their cyber risks"[7]), or how the information collected in response to the RFI could possibly interplay with that important effort and others.

[7] *See* DHS, *DHS Launches the C³ Voluntary Program, A Public-Private Partnership to Strengthen Critical Infrastructure Cybersecurity* (last visited Mar. 31, 2014), *available at* https://www.dhs.gov/blog/2014/02/12/dhs-launches-c%C2%B3-voluntary-program.

TIA can only guess what the information collected in this will be specifically used for, past providing "broadly scalable cyber security solutions at an affordable cost" to SMBs.

In short, TIA is unclear as to what the RFI *is* intended for. We strongly urge that, before moving forward further, DHS provide a full explanation as to why it is requesting such information and how it intends to use it.

c. *TIA urges for DHS' consideration of the existing market incentives and the public-private partnership model.*

In Section 3 of the RFI, DHS poses eight broad questions that address, among other topics, the availability of cybersecurity solutions to SMBs at affordable prices, DHS' role in determining what "adoption" of the NIST Cybersecurity Framework is for SMBs, and whether there technical or policy impediments that inhibit the marketplace from providing cyber security solutions at a low, affordable price for SMBs.

First, DHS may find more than ample information, from across industries to the company-specific level, in the publicly-posted submissions from hundreds of stakeholders that took part in NIST's transparent process.[8]

Second, generally, TIA urges that DHS recognize that, today, very strong market-based incentives exist throughout and across critical infrastructure sectors, including SMBs. The market, and not a government agency, naturally determines whether "a viable marketplace for providing cyber security services at a low, affordable price for SMBs in support of the NIST Cybersecurity Framework" exists. TIA member equipment manufacturers and suppliers already spend billions of dollars on efforts to responsively address cyber-based resiliency threats in order to best competitors and ensure continuing business relationships. These programs are very often based on open, international, and consensus-based standards, including, but not

[8] *See* http://www.nist.gov/cyberframework/cybersecurity-framework-rfi.cfm.

limited to, the Open Group Trusted Technology Forum ("OTTF")[9] and SAFECode,[10] among others. We have emphasized that there is no universal solution that will accommodate all stakeholders in their efforts to improve resiliency to cyber-based attacks (or help in assessing the adequacy of these efforts). We strongly encourage

TIA also believes that efforts to improve cybersecurity must leverage the successful public-private partnership model as an effective tool for collaboration on addressing current and emerging threats. Public-private partnerships have been recognized as the basis for the cyber defense of critical infrastructure and cybersecurity policy for the last decade.[11] 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 DHS and other United States government agencies leverage and augment existing public-private partnerships previously mentioned in this filing, as well as the National Cybersecurity Center of Excellence (NCCoE) and the Small Business Administration's *Cybersecurity for Small Businesses* effort, among others.

Building on the above, TIA notes that an important factor that drives cybersecurity investment incentives among business sectors is the degree to which that sector is competitive. Coupled with the critical nature of a business sector, increased competition will drive heightened

---

9 OTTF is a collaborative public-private initiative that includes U.S. government participation, and encourages governments worldwide to participate alongside representatives from commercial technology companies. This initiative was established to promote the adoption of best practices to improve the security and integrity of products as they move through the global supply chain. The forum has established a framework that outlines best practices to improve the integrity of every aspect of the product development lifecycle. The OTTF also intends to develop an accreditation process to go with the framework to ensure a practitioner has adopted the practices in accordance with the framework, and has encouraged governments to participate by submitting their assurance requirements.

10 SAFECode is a global, industry-led initiative whose mission is to advance the use of effective software assurance methods, thus addressing concerns about the manufacturing process for ICT products. It seeks to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services. This initiative has defined a framework for software supply chain integrity that provides a common taxonomy for evaluating software engineering risks, and outlines the role that industry participants should play in addressing those risks.

11 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.

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

cybersecurity investment mainly due to market differentiation needs discussed above. For example, the banking and telecommunications business sectors, which are highly competitive and have many market entrants, will have an increased incentive to make cybersecurity investments over other business sectors, such as the water or railroad business sectors, which have relatively less market entrants. In short, competition drives investment and innovation. Competition also enables wide distribution of points of control under many entities and a diversity of approaches to defend against cyber attack, lowering the potential for widespread harm from cyber attack.

d. Education and public awareness are crucial to improving cybersecurity resiliency for all stakeholders, including SMBs.

Finally, TIA notes the importance of education and public awareness in efforts to improve resiliency to cyber-based attacks. These educational efforts, ideally coordinated across the government, will aid SMBs in understanding cybersecurity threats, increase awareness of existing resources available from the government to help, and help explain how these resources can be best utilized (*e.g.*, how to use the NIST Framework). In addition, it is well-documented that a large majority of successful cybersecurity attacks can be prevented through better cyber "hygiene." TIA strongly supports Federal efforts to increase awareness of cybersecurity issues among both institutional users and the general public. 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. TIA has long noted its support the CSRIC-based recommendation that network operators and service providers educate the customers on important steps that should be taken, from the use of adequate passwords to encryption of data.[12]

[12] *See* CSRIC Working Group 2A Report. *Cybersecurity Best Practices* (Mar. 14, 2011), *available at* http://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf.

III. Conclusion

TIA urges the consideration of the above positions. The ICT manufacturing and vendor community stands ready to work with all government actors to improve resiliency to cyber-based attacks.

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
703.907.7700

April 4, 2014