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

January 17, 2014

Filed electronically via www.regulations.gov

Defense Acquisition Regulations System
Attn: Mr. Dustin Pitsch
OUSD (AT&L) DPAP/DARS
Room 3B855
3060 Defense Pentagon
Washington, DC 20301–3060

Re: Comments of the Telecommunications Industry Association to the Department of Defense's *Defense Federal Acquisition Regulation Supplement: Requirements Relating to Supply Chain Risk (DFARS Case 2012-D050)*

I. Introduction and Statement of Interest

The Telecommunications Industry Association ("TIA") hereby submits comments to the Department of Defense ("DoD") on its proposed amendments to the Defense Federal Acquisition Regulation Supplement ("DFARS") to implement section 806 of the National Defense Authorization Act for Fiscal Year (FY) 2011, as amended by the NDAA for FY 2013 ("NDAA"),[1] relating to supply chain risk.[2] TIA appreciates the opportunity to comment on the impact of supply chain risk in specified types of procurements related to national security systems.

---

[1] National Defense Authorization Act for Fiscal Year 2013, H.R. 4310, P.L. 112-239.

[2] DoD, *Defense Federal Acquisition Regulation Supplement: Requirements Relating to Supply Chain Risk (DFARS Case 2012-D050)*, 78 Fed. Reg. 69267 -69273 (Nov. 18, 2013) ("Interim Rule").

The Interim Rule impacts TIA's membership because it alters rules covering solicitations and contracts for the development or delivery of any information technology, including solicitations and contracts for commercial information and communications technology ("ICT") items and commercial-off-the-shelf ("COTS") items supplied to the DoD and used in national security systems ("NSS"). TIA represents approximately 500 ICT manufacturer, vendor, and supplier companies and organizations in developing standards, government affairs, and market intelligence. TIA member companies produce ICT products and systems, create information security-related technologies, and provide ICT services information systems, or components of information systems. These products and services innovatively serve, among many important entities, the Department of Defense. 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 and Information Technology Sector Coordinating Councils, and the Federal Communications Commission's Communications Security, Reliability and Interoperability Council ("CSRIC").[3]

II. TIA Input on DoD's Interim Supply Chain Security Rule

a. *DoD should provide clarification as to what is expected of contractors and vendors of information technology, including the role of current certification programs.*

TIA believes that, in its current form, the Interim Rule adds uncertainty to the NSS vendors regarding the DoD's assessment of supply chain risk. While adding sections to Parts 208, 212, and 215 that add supply chain risk factors to DoD evaluations on sufficiency of bids, the Interim Rule also states that changes are not necessarily needed to the existing behaviors for relevant organizations.[4] Furthermore, the Interim Rule states that contractors must maintain controls in

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

[4] For example, DoD states that these rules "…do[] not require any specific reporting, recordkeeping or compliance requirements" and "do[] not require contractors to deploy additional supply chain risk protections, but leaves it up to the individual contractors to take the steps they think are necessary to maintain existing or otherwise

the provision of supplies and services to minimize supply chain risk.[5] This ambiguity does not provide a high level of certainty as to the effect of the Interim Rule as it moves towards finalization. NSS equipment manufacturers and suppliers already spend billions of dollars both on rigorous internal supply chain verification, and in complying with DoD customer requirements. These dynamic and resilient supply chain integrity programs are based on international consensus standards, including, but not limited to, the Open Group Trusted Technology Forum ("OTTF"),[6] SAFECode,[7] and the Common Criteria ("CC").[8]

DoD is strongly encouraged to ensure that new supply chain risk rules do not alter the healthy environment described above that assures supply chain security, as well avoids the creation of unneeded duplication of certifications of these important assurance efforts, by affirming that the Interim Rule shall not impact the duties of contactors and vendors in assessing relevant procurements related to NSS.

---

required safeguards and countermeasures as necessary for their own particular industrial methods to protect their supply chain." *See* Interim Rule at 69269.

[5] *See* 48 C.F.R. 252.239-7018(b).

[6] 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.

[7] 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.

[8] The Common Criteria for Information Technology Security Evaluation (ISO/IEC-15408) is both an ISO standard and a multi-lateral recognition arrangement among the national security agencies of 26 countries, including the NSA as the U.S. representative. Pursuant to the Common Criteria Recognition Arrangement (CCRA), it has recently authorized a pilot on supply chain assurance to address the supply chain issue. CC certification is required by the Committee on National Security Systems (CNSS) for the use of certain key products in U.S. National Security Systems. As the U.S. tech industry builds-once-and-sells-globally, those same CC-certified products are used in private sector systems.

b. ***DoD should ensure a means of fair assessments and an impartial process for addressing concerns.***

We urge that the Interim Rule reinforce the need for reasonable assessments of supply chain risk[9] consistent with the less intrusive measures test in section 239.7304(b)(2), along with a fair opportunity pre- and post-exclusion for concerns to be addressed by the contractor or vendor at issue, consistent with the related discussion below.

First, DoD should clarify what it believes are less intrusive measures under section 239.7304(b)(1)(2). In order to prevent the Interim Rule from impeding the use of commercial technology (including COTS items) in NSS, which ultimately benefits DoD, TIA recommends that the DoD provide wide discretion to the judgment of manufacturers in their use of industry standards and internal processes to meet its supply chain risk goals. That is because companies that contract with and vend to the federal government (in particular DoD) consider attaining and maintaining the proper level of trust to be of upmost importance.

Second, TIA strongly urges DoD to revise sections 239.7304 and 239.7304 of the Interim Rule to require timely notification to an organization of that organization's status as part of this process, consistent with the NDAA, to such organizations based on the following:

- Notification to organizations of their potential status, pre-exclusion, will allow organizations to rectify instances before DoD makes a determination based on incorrect or insufficient information, ensuring fairness to the organization and benefitting DoD by enhancing fairness in competition for contracts.

[9] In implementing this approach, we ask that the DoD be mindful that the demands of market competition in commercial ICT products limit the time available to wait for a DoD assessment.

- In the event an authorized individual has determined that a legitimate insufficiency exists within an organization's supply chain, notification to excluded organizations of their post-exclusion status and the reasons for exclusion will allow organizations to take steps to remedy those flaws before future opportunities. This would benefit that organization and its customers generally, as well as DoD, should the organization's supply chain be assured at a later time.

While DoD's implementation of Section 806 in section 239.7304 (Determination and notification) includes steps to prevent the arbitrary exclusion of an organization on the basis of an insufficient supply chain security, timely notification of pre- and post-exclusion status to the organization itself is not required as part of this process. Yet such notification should be part of the process to ensure competitive fairness.

Furthermore, limitations on alternative resolutions to review exclusions where authorized individuals limit "the disclosure of information relating to the basis for carrying out any of the authorized actions" under paragraphs (a) through (c) of section 239.7305, such as the limitation on bid protests, further underscores the need to provide this information to excluded organizations in order to ensure fairness in competition.

c. *DoD's process for determining insufficiency under the Interim Rule should clearly define its standard of review.*

Noting our above-discussed input regarding the Interim Rule's process for denying NSS equipment contracts needing improved notice of exclusion and fair assessments, TIA strongly recommends that DoD revisit the Interim Rule to clarify its standard of review. For example, in proposed section 239.7304 (Determination and notification), it is provided that an exclusion under 239.7305 may occur when it is determined that, among other factors, "[l]ess intrusive measures are not reasonably available to reduce such supply chain risk."[10] However, at no point in the Interim Rule is clarity provided on what this language is defined as or what an authorized individual should refer to in order to gauge what "less intrusive measures" are and whether they are "not reasonably available." We therefore urge that DoD provide definitions of these ambiguous terms, which should be proposed for public input. Such clarity will greatly aid authorized individuals in the performance of their duties by providing an objective standard of review, as well as stakeholders seeking to understand the process and to comply with DFARS.

[10] *See* 47 C.F.R. 239.7304(b)(2).

III. Conclusion

TIA urges DoD's consideration of the above positions as DoD implements section 806, and we urge the consideration of the above positions. The ICT manufacturing and vendor community stands ready to work with DoD and all other government actors to improve supply chain security.

Respectfully submitted,

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

By: */s/ Danielle Coffey*

Danielle Coffey
Vice President & General Counsel, Government Affairs

Brian Scarpelli
Senior Manager, Government Affairs

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

January 17, 2013