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

July 15, 2013

Via Electronic Filing

Defense Acquisition Regulations System
Attn: Ms. Meredith Murphy
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: Detection and Avoidance of Counterfeit Electronic Parts* (DFARS Case 2012–D055)

I. Introduction and Statement of Interest

The Telecommunications Industry Association ("TIA") hereby submits comment on the Department of Defense ("DoD") on its proposed amendments to the Defense Federal Acquisition Regulation Supplement ("DFARS"), in partial implementation of a section of the National Defense Authorization Act for Fiscal Year 2012, and a section of the National Defense Authorization Act for Fiscal Year 2013 ("NDAA"),[1] relating to the detection and avoidance of counterfeit electronic parts.[2] TIA appreciates the need to decrease the probability of counterfeit items across the DoD. While the threat of counterfeit electronics is increasingly being taken seriously in the key issues of acquisition and oversight due, it is also important that DoD does not isolate itself from innovative technology.

---

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

[2] DHS, *Review and Revision of the National Infrastructure Protection Plan*, Notice and request for comments, 78 Fed. Reg. 34020–34024 (Jun. 6, 2013) ("RFC").

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 PPD-21 and the accompanying Executive Order 13636.[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 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 released cybersecurity policy recommendations for critical infrastructure and the global supply chain that have shaped our views below, and that we urge NIST to review.[6]

---

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

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

[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).

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.[7]

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.[8] 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 (TAGs) 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 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.[9]

---

[7] 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* http://www.tiaonline.org/standards_/about/documents/STAR_2012_Web.pdf. TIA standards are available from IHS, Inc. *See* http://www.ihs.com/.

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

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

II. TIA Input on Proposed Changes to the DoD Detection and Avoidance of Counterfeit Electronic Parts Supplement

As DoD moves forward with its implementation of the NDAA, we urge the careful consideration of the following principles:

Clear, Accurate, and Uniform Definitions and Accountability are Key. We offer the following regarding proposed DoD DFARS definitions:

- Defining "counterfeit":
  - TIA supports defining counterfeit parts as those which are produced or altered to resemble a product without authority or right to do so, with the intent to mislead or defraud by presenting the imitation as original or genuine.[10]
  - DoD should remove references to "substitute" equipment because genuine replacement ICT equipment may well be "identified [or] marked… by a source other than the part's legally authorized source." We believe that this could have the effect of excluding legitimate substitutes for or alternative to original equipment manufacturer ("OEM") parts due to such circumstances as a legally authorized source no longer producing the needed ICT equipment. The definition could likewise be interpreted to unnecessarily exclude certain Commercial-Off-The-Shelf ("COTS") items, which would effectively, and improperly, treat such items as non-genuine.
  - DoD should ensure that its definitions of counterfeit do not include ICT which is misrepresented at no fault of its manufacturer and due to supplier error.
- Defining a "legally authorized source"[11]:
  - The phrasing is ambiguous and could possibly be construed in the future to mean only the design of the OEM, or be construed to operate as a freeze in time, foreclosing any future ICT equipment not a "current design activity."
  - Liability for misrepresentation to the end-user of meeting the performance requirements for the intended use should be applied the only to the one responsible for making such an erroneous statement. Any statements by authorized resellers should not create liability to the OEM if it did not directly control the reseller.
  - The DoD should also recognize that the actions of an authorized reseller in no way creates a legal liability for the OEM manufacturer where the reseller integrates third party components to configure or customize the product at the direction of the DoD.

[10] We believe this to be consistent with the Lanham Act, which defines a counterfeit as "a spurious mark which is identical with, or substantially indistinguishable from, a registered mark." 15 U.S.C. § 1127.

[11] We note that the current proposed rules would apply to contractors subject to Cost Accounting Standards, as defined in 41 C.F.R. § 1502.

In addition, DoD should ensure that it applies the DFARS in a fair and integrated manner that will avoid undue preferences. For example, TIA sees no reason for an exception to small business entities that is currently proposed.

The ICT Supply Chain is Global. Governments and industry alike are reasonably concerned about supply chain security. The global ICT industry depends on a globally flexible supply chain, characterized by intense competition and fluctuation in price and supply of different inputs. Because products and components may be designed, manufactured, and assembled in different locations, it would be impractical for the commercial sector to eliminate the use of global resources or a distributed supply chain model. The focus of any product security concerns must always be on whether the product is secure – not the country of origin.

Strong Market Incentives Exist. Companies have strong market-based incentives to insure that their products – and the networks they support – are safe, reliable, and secure. ICT companies already spend billions of dollars both on rigorous internal product verification, and in complying with customer requirements. Moreover, warranty terms provide a legal obligation to ensure products perform as designed.

Public-Private Partnerships and Industry Efforts are Underway. Aside from company-internal measures, efforts are being undertaken both in conjunction with industry competitors, and as public-private partnerships with government entities. Examples include:

- **Open Group Trusted Technology Forum (OTTF).** 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.

- **SAFECode.** 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.
- **Common Criteria (CC).** 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.
- **AS5553 Standard.** The AS5553 Standard on Fraudulent / Counterfeit Electronic Parts – Avoidance, Detection, Mitigation, and Disposition was developed by the G-19 committee of SAE International. It was first issued in 2009, but recently revised in 2013. The standard provides uniform requirements, practices and methods to mitigate the risk of receiving and installing fraudulent or counterfeit electronic parts. The DoD and NASA have also adopted this standard for their own use.
- **ISO / IEC 27000 Information Security Management Systems (ISMS) Standards.** The ISO / IEC 27000 series is a collection of standards that provides best practice recommendations on information security management, risks, and controls within a larger ISMS context. It includes general guidelines for risk management, as well as

specific standards for cybersecurity, network security, application security, and incident management.

Standards-Based Approaches Provide Meaningful Alternatives to Regulation. TIA supports the use of a standard-based approach (as noted above) that is technology neutral and affords industry with a variety of choices that enable flexibility in implementation. The best approach to addressing concerns about supply chain vulnerability is one that comes from the bottom-up rather than through rigid and potentially harmful government regulations.

Effective Mitigation of Counterfeit ICT from the Acquisition Process Requires a Systemic Focus. Systemic approaches focused on risk analysis – including how networks are configured and products are used – are more effective than regulating how products are designed or manufactured. This is why, for example, the recent Executive Order 13636[12] recognized that commercial ICT products and services themselves do not constitute "critical infrastructure." A self-regulated model allows the parties with the most knowledge of the ICT supply chain process to evaluate current practices and provide recommendations on how to minimize risk.

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 DFARS changes reinforce the need for reasonable assessments of a contractor's counterfeit electronic part avoidance and detection system along with a fair opportunity for concerns to be addressed by the contractor or vendor at issue. 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 order not to impede the use of commercial technology in defense systems, which ultimately benefits DoD, the Agency should give wide discretion to the judgment of manufacturers in their use of industry standards and internal processes to meet these goals. In the event that additional information is required to make an accurate and

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

complete assessment, DoD should provide discretion to procurement staff to provide short term waivers for the introduction of new technology or products.

Global Cooperation is Required. A U.S. policy will effectively serve as a global standard. Therefore, the U.S. should not enact U.S.-only policies that would restrict trade in ICT equipment. Other countries have cited similar concerns regarding foreign ICT equipment and are currently considering trade restrictive measures. U.S. global economic competitiveness could be severely affected by other export markets adopting similar restrictive policies.

Liability Assurances. 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). For this reason TIA supports the cost recovery exception listed.

However the preamble states that this relief is available if (i) a contractor has a DoD-approved operational system to detect and avoid counterfeit parts; or the suspect counterfeit parts were provided as Government-furnished property, and (ii) the contractor has provided timely notice to the Government; while the text of the proposed rule is more limiting in that it relieves the disallowance only where the contractor meets all three criteria, which are that the contractor (i) maintains a DoD-approved counterfeit parts compliance system, (ii) receives the counterfeit parts as Government-furnished property, and (iii) provides timely notice. TIA urges for DoD to clarify the text to allow for relief when a contractor maintains a DoD-approved counterfeit parts compliance system *or* receives the counterfeit parts as Government-furnished property, and provides timely notice.

Expertise as Part of the Acquisition Process, and End-User Education. A large challenge for reform in the acquisition process generally will be to ensure that security 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 the avoidance of counterfeit ICT, as many vulnerabilities are already known and may result from conscious decisions to purchase from unauthorized sources, making these threats relatively easily preventable.

III. Conclusion

TIA supports DoD in its implementation of the DFARS, 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 the detection of counterfeit ICT in the supply chain.

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
10 G Street N.E.
Suite 550
Washington, D.C. 20002
(202) 346-3240

July 15, 2013