TELECOMMUNICATIONS INDUSTRY ASSOCIATION
ADVANCING GLOBAL COMMUNICATIONS

1320 N. Courthouse Rd., Suite 200
Arlington, VA 22201 USA
www.tiaonline.org

Tel: +1.703.907.7700
Fax: +1.703.907.7727

Draft TIA Public Statement – Detection and Avoidance of Counterfeit Electronic Parts-Further Implementation

March 27, 2014

Brian Scarpelli
Telecommunications Industry Association (TIA)
d: 703.907.7714| m: 517.507.1446
BScarpelli@tiaonline.org | tiaonline.org

Thank you. My name is Brian Scarpelli of the Telecommunications Industry Association.

As background on TIA, we are a DC-based trade association representing the information and communication technology (ICT) manufacturer, vendor, and supplier community through 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 used in countless projects contracted with DoD. We congratulate DoD on convening this forum to hear public views on implementation of the requirement for detection and avoidance of counterfeit electronic parts and in particular trusted suppliers.

For companies that 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 may 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 complete assessment, DoD should provide discretion to procurement staff to provide short term waivers for the introduction of new technology or products. TIA submitted more detailed comments to the DoD on its proposed changes relating to trusted sources, including on the proposed definitions of "counterfeit" and "legally authorized source," that we urge the consideration of.

We would also like to emphasize that the 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.

Companies already have strong market-based incentives to insure that their products are genuine, safe, reliable, and secure. ICT companies already spend billions of dollars both on rigorous internal product verification, and in complying with customer requirements. Also, warranty terms provide a legal obligation to ensure products perform as designed. In addition, numerous efforts are already underway, both in conjunction with industry competitors and as public-private partnerships with government entities. Examples on ongoing efforts include the Open Group Trusted Technology Forum (OTTF), the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408), and the AS5553 Standard on Fraudulent / Counterfeit Electronic Parts developed by the G-19 committee of SAE International, among others. DoD should ensure that any changes made to address counterfeit electronic parts does not negatively alter this environment.

Finally, TIA emphasizes 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.

In conclusion we thank the DoD for convening this forum to hear public views on implementation of the requirement for detection and avoidance of counterfeit electronic parts.