



May 20, 2013

The Honorable Fred Upton  
U.S. House of Representatives  
2183 Rayburn House Office Building  
Washington, DC 20515

The Honorable Henry Waxman  
U.S. House of Representatives  
2204 Rayburn House Office Building  
Washington, DC 20515

The Honorable Greg Walden  
U.S. House of Representatives  
2182 Rayburn House Office Building  
Washington, DC 20515

The Honorable Anna Eshoo  
U.S. House of Representatives  
241 Cannon House Office Building  
Washington, DC 20515

Dear Chairmen and Ranking Members:

The Telecommunications Industry Association (TIA), the leading trade association for global manufacturers, vendors, and suppliers of information and communications technology, wishes to thank you for holding cybersecurity hearings this week. TIA and its member companies are committed to ensuring that ICT products and technologies are secure, reliable, and able to adapt to ever-evolving threats. As the Subcommittee on Communications and Technology prepares to discuss the security of the communications supply chain, we urge you to consider the following principles.

*The ICT Supply Chain is Global.* Governments and the private sector – whether in the United States or elsewhere – are reasonably concerned about supply chain security. However, the global ICT industry depends on a globally flexible supply chain, characterized by intense competition and fluctuation in price and supply of different inputs. Products – and their components – may be designed, manufactured, and assembled in different locations. Indeed, market demands are such that it would be impractical for the commercial sector to eliminate the use of global resources or a distributed supply chain model. Therefore, the focus of any product security concerns must always be on whether the product is secure.

*Strong Market Incentives Exist.* The ICT industry itself is very interested in maintaining the security and integrity of its supply chain, since companies have strong market-based incentives to insure that their products – and the networks they support – are safe, reliable, and secure. Indeed, ICT companies already spend billions of dollars both on rigorous internal product verification, and in complying with customer requirements.

*Public-Private Partnerships and Industry Efforts are Underway.* Industry members have taken proactive steps to form initiatives aimed at dealing with the issues involving the global supply chain in ways that are most amenable to ensuring supply chain security. These efforts are being undertaken both in conjunction with industry competitors, and as public-private partnerships with government entities. Examples include SAFECode and the Open Trusted Technology Forum (see appendix).

*Standards-Based Approaches are Essential.* The public-private efforts described above demonstrate the right approach to supply chain security – namely, by developing best practices and standards. These and other standards-based approaches – including the Common Criteria for Information Technology Security Evaluation, the AS5553 Standard on Fraudulent / Counterfeit Products, and the ISO 27000 series of

standards on information security management systems (see appendix) represent more constructive approaches to addressing ICT product security than would micro-management of the product development process. Indeed, the best approach to addressing concerns about supply chain vulnerability is one that comes from the bottom-up rather than the implementation of rigid and potentially harmful government regulations.

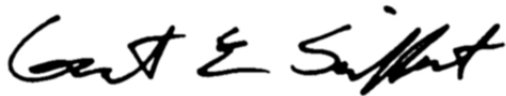
*Effective Cybersecurity Requires a Systemic Focus.* An improved cybersecurity posture is best achieved through systemic approaches focused on risk analysis – including how networks are configured and products are *used* – rather than by regulating how products are designed or manufactured. Indeed, in adopting a risk-based approach to critical infrastructure security, the recent executive order explicitly recognized that commercial ICT products and services themselves do not constitute “critical infrastructure.” Meanwhile, 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.

*Global Cooperation is Required.* The United States must move cautiously in this area since U.S. policy will effectively serve as a global standard. Therefore, the U.S. should not enact U.S.-only cybersecurity policies that would restrict trade in telecommunications equipment imported to, or exported from, other countries that are part of the global trading system. Other countries have cited similar concerns regarding foreign ICT equipment and are currently considering trade restrictive measures. India, for example, has recently taken steps towards the implementation of a Preferential Market Access (PMA) policy that requires a percentage of ICT products to be manufactured domestically – essentially attempting to impose industrial policy in the name of security. U.S. global economic competitiveness could be severely affected by other export markets adopting similar restrictive policies.

\*\*\*\*

TIA thanks you again, and we look forward to working with you on these important issues. For more information, please contact Danielle Coffey at (703)-907-7734 or by email at [dcoffey@tiaonline.org](mailto:dcoffey@tiaonline.org).

Sincerely,



Grant E. Seiffert  
President

Enc: Appendix – Public-Private Partnerships, Best Practices, and Standards

## Appendix

### Public-Private Partnerships, Best Practices, and Standards

**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.

**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.