Information Technology Industry Council

Written Testimony of

Dean C. Garfield

President & CEO, Information Technology Industry Council (ITI)

Before the

Committee on Energy and Commerce

Subcommittee on Communications and Technology

U.S. House of Representatives

Cybersecurity: An Examination of the Communications Supply Chain

May 21, 2013

Dean C. Garfield Testimony
Cybersecurity: An Examination of the Communications Supply Chain
May 21, 2013

Chairman Walden, Ranking Member Eshoo, and members of the subcommittee, thank you for the opportunity to testify today. I am Dean Garfield, President and CEO of the Information Technology Industry Council (ITI), and I am pleased to testify before the Communications and Technology Subcommittee on the important topic of cybersecurity and the communications supply chain. The Chairman and Ranking Member are well-regarded forward-thinking policy leaders on many issues that matter to our industry, and we welcome your interest and engagement on this subject.

ITI represents the world's leading technology companies from all corners of the information and communications technology (ICT) sector, including hardware, software, and services. Almost all of our members service the global market and have complex supply chains spanning multiple countries where products and services are developed, made, assembled, and distributed across the world. Supply-chain security practices are critical to our members' success—the protection of our customers, our brands, and our intellectual property are essential components of our business and our ability to grow and innovate in the future. Consequently, ITI has been a leading voice in advocating a balanced policy approach to mitigate risks and ensure the integrity of ICT supply chains.

I will focus my testimony today on four areas: (1) The considerable benefits of global supply chains to ICT companies and their customers, including the government; (2) the ICT supply-chain risks we recommend government to focus on; (3) how the private sector manages and mitigates supply-chain risks; and (4) how the government can be an effective and valuable partner in supply-chain integrity.

Ultimately our conclusion is that government has an important role to play, but government policies must be carefully calibrated to the risks faced by government or industry customers, and should not supplant the panoply of risk mitigation practices being used by ICT companies. Government policies also must be globally workable. Acting precipitously has the potential to create a check-the-box compliance regime and decrease supply-chain security over the long-run, particularly if policies regulate and mandate behavior throughout the global ICT supply chain. Unintended consequences could include deterring companies from taking swift action to respond to risk (for example, out of fear of violating a regulation that requires them to take a prescribed action when building their products), or deterring them from developing new practices to address new risks by increasing the cost of innovation.

We note that the government already is involved in a constructive way, such as by supporting global, industry-led voluntary consensus supply chain security standards activities and working with industry through the Executive Order to improve government ICT procurement practices. Greater cyber-threat information sharing is also critical—this is addressed in part in the Executive Order, but further Congressional action is needed.

Global ICT Supply Chains Benefit All Customers, Including the Government

ICT supply chains are globalized because the global system benefits all of us, including government purchasers. Most ICT acquisitions, whether made by government or industry, are fundamentally purchasing "commercial-off-the-shelf" (COTS) products. The U.S. government has a mandated preference for purchasing COTS ICT products, including for the Department of Defense. This decision was based on a calculation that in many cases the benefits to the government of using COTS hardware and software – including cost, functionality AND security – outweigh the

benefits of using custom-developed products.

COTS ICT products are designed with a global audience in mind and are made available to the general public, whether individuals or organizations, and include software, such as operating systems and databases, and components and hardware, such as semiconductors, laptops, routers, and smartphones. In short, these are products we in industry and government use every day. Nearly all COTS ICT products—from U.S. and non-U.S. based companies—rely on global supply chains. By researching, developing, and manufacturing globally, COTS ICT companies gain global talent, resiliency/redundancy of suppliers, high-quality low-cost inputs, and manufacturing efficiencies. This leads to affordable, leading-edge technology products that enhance our country's productivity and competitiveness. In short, reliance on COTS rather than government-specific solutions not only cuts costs and boosts efficiency, but increases security.

It is also worth noting that, for U.S.-based companies, global supply chains have become absolutely essential to maintain a competitive edge in the global marketplace. Consumers increasingly demand 24/7/365 operations and production capacity. Global supply chains effectively keep a company's research, development, manufacturing, and maintenance of products and services operating on a 24/7/365 basis. Global supply chains are not just about company success, but also competitiveness and, therefore, survival.

ICT Industry Activities to Manage Global Supply-Chain Security Risks

Within any supply chain, as with any activity, there are risks. Risks exist during product development, manufacturing and shipment. Because these risks threaten the core of ICT businesses (our products) our sector is highly motivated to combat these risks with the same innovative focus we apply to our own product development. For ICT companies, the primary focus is the integrity, reliability and functionality of the product at hand. To advance these goals, companies assess a range of risks, including evaluating the security properties of inbound components and products as well processes and testing throughout the products lifecycle. These processes help guard against the risks of both malicious and unintentional vulnerabilities that may be inserted during the product development process.

The ICT industry manages supply-chain security risks in numerous ways. It is important to note that due to the various types of risk and their impact on such a wide variety of products in the communications sector, there is no single activity that protects all global ICT products. Instead, ICT companies utilize many different practices in concert based on an assessment of risk, which can be unique to each company's situation.

Company-specific activities: Individual ICT companies have been managing supply-chain security risks for years, and as a result, they have deep expertise on the practices that are best suited to mitigate their particular risks. Our companies undertake a number of activities to secure their supply chains.

- Product development practices. These practices span from product concept to completion. They include providing security training for product developers, defining security requirements at the outset of product development, identifying and addressing potential threats in the early design phases (e.g., threat modeling and mitigation planning), teaching and instilling secure coding practices, teaching and instilling secure code handling practices, conducting product testing to validate that security practices have been met, and security documentation.
- Purchasing from authorized suppliers, using contracts as enforcement. One way in which the technology

industry seeks to ensure supply chain integrity is through the use of authorized distributors and/or resellers. In an authorized relationship, each supplier identifies and qualifies their authorized distributors and/or resellers using a broad set of criteria, which includes legal and regulatory compliance, long-term business viability, quality systems, order placement and fulfillment processes, customer support policies, and other contractual requirements. Contracts provide enforcement mechanisms and a range of potential actions, from remediation, to termination, to legal action. In addition, suppliers periodically audit their distributors to ensure product management and contractual provisions are properly executed. Similarly, purchasing only from authorized distributors and resellers is one simple way that the U.S. government can gain higher levels of assurance than if it chooses to purchase from unauthorized sources.

Industry-wide standards activities: More recently, industry has been working together in multiple forums to develop common best practices, controls, and standards for supply-chain risk management. Several industry-wide standards and best practices address ICT supply-chain risks. Our companies contribute to developing such standards on a global, voluntary, and consensus basis through a range of organizations. Examples of supply-chain security standards include a variety of International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standards, including:

- ISO/IEC 15408, which serves as the basis for the Common Criteria, the global IT security certification arrangement. A pilot is underway to incorporate supply-chain risks in the Common Criteria evaluations of IT products. It is important to note that the Common Criteria is an agreement among the governments of 26 mostly developed nations. The U.S. is represented in the Common Criteria by the National Information Assurance Partnership, which is led by the National Security Agency; and
- The ISO/IEC 27000 risk management framework, which will include a component under development to address supply-chain security (27036, information security for supplier security).

In addition, other activities include:

- The Software Assurance Forum for Excellence in Code (SAFECode) is a non-profit organization exclusively dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. SAFECode is a global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services.
- The Open Group Trusted Technology Forum (OTTF) is an industry-led global standards initiative that aims to shape global procurement strategies and best practices that help to reduce threats and vulnerabilities in the global supply chain. The U.S. Department of Defense is a member of the OTTF.
- SAE-AS5553, "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition" is an industry best practice.

The standards efforts above are global, with participation and contributions from companies from all over the world. In addition, many of them include government participation—not as dominant players, but as distinct stakeholders with interests in the outcome.

Again, it is important to stress there is no one-size-fits-all "supply-chain security standard" or set of practices applicable across the board. The security practices a particular company chooses depend on its products, services,

markets, and business methods. In addition, industry continually updates existing standards or establishes new standardization efforts addressing emerging cybersecurity risk concerns. Thus, the government should recognize and support these activities, but not mandate any one standard, approach, or activity. Such an inflexible approach would likely divert resources away from addressing emerging risks and challenges, thereby decreasing security. Given the substantial time and resources the government would need to devote to identifying standards and writing them into contracts, the reality is that any government –required standards will be static, rather than evolving to address changing threats. Security standards evolve as new threats and vulnerabilities emerge, and new products and technologies emerge as well. *Today's best practice can be outdated tomorrow.*

How the Government Can Be Helpful

As policymakers, you are increasingly and rightfully interested in the security of the software and hardware procured by government agencies and critical infrastructure (CI) sectors generally. This increased government focus is putting new expectations on industry's supply-chain risk management activities. The single largest thing that government can do to address its concerns regarding government systems is ensure that all ICT products are purchased from authorized sources.

In recent years we have seen a rush to legislation and regulation, and to interfere with standards development. There have been dozens of supply-chain related bills and provisions in legislation, including in successive National Defense Authorization Acts, and most recently, in the continuing funding resolution that was enacted just last month. More are expected. Various agencies, including the Department of Defense, the Department of Homeland Security, the National Institute of Standards and Technology, the Office of Management and Budget, the General Services Administration, and the Department of Commerce are working on proposals and programs alone or at an interagency level to address supply-chain concerns.

We support the government's efforts to better understand and improve the security of U.S. federal and telecommunications systems and networks. We consider ourselves partners in this shared effort. We certainly understand the urge to act as fast as possible, but also believe an important rule to follow is based on the old adage "first, do no harm." That starts with ensuring that proposed solutions to perceived supply-chain security concerns are based on sound risk management practices. In addition, we believe the best solutions are ones that acknowledge the global nature of supply chains and therefore work in concert with the sophisticated processes and procedures industry has been implementing for decades.

Some recent proposals, however, have tended to:

- Insist on a regulatory system;
- Include U.S. Government-specific requirements or approaches (such as new standards written by the government for industry-wide use);
- Not allow for private-sector leadership and collaboration;
- Include technology mandates that artificially pick winners and losers;
- Include burdensome procurement requirements that go beyond federal procurement and into mandates on industry;
- Focus solely on vendors' design and building of products, and not on government users' procurement and implementation;

- Focus on specific supply-chain vulnerabilities, and not supply-chain risk management; and
- Focus on where technology is developed, rather than how, which fails to evaluate the security of the product, gives a false sense of security, and is incompatible with global supply-chain models.

Most concerning is that many of these proposals have the unintended consequence of decreasing, not increasing, cybersecurity, because industry needs the flexibility to innovate in response to actual and emerging threats. U.S.-specific regulations and practices could impede U.S.-based ICT companies' ability to compete in the global marketplace. For example, measures that would require companies to build U.S.-specific products, in addition to products for the global market, would have an immeasurable negative competitive impact. Second, other countries, interpreting our actions as an attempt to create barriers to foreign entry into U.S. markets, will emulate such proposals and pursue their own domestic requirements. A "race to the bottom" of a myriad of national requirements would ensue, leading to a patchwork of conflicting requirements from various governments, balkanizing the global ICT marketplace. This would significantly diminish the benefits that our customers derive from our massive research and development (R&D) investments – which we can only afford if we can expect the commensurate return on investment that comes from serving a global marketplace. These benefits include fast paced innovation (new products with new and useful features), global interoperability, low cost, and – most importantly – constantly improved product security.

Unfortunately, we are already seeing other countries propose market access restrictions under a banner of supply-chain security. We fear a contagion effect from these types of approaches that will undermine U.S. cybersecurity and U.S.-based company success in global markets.

U.S. government efforts should focus on:

- Creating incentives for the effective implementation of the President's February 12 cybersecurity Executive Order to continue. The Executive Order directs the General Services Administration and the Department of Defense to study the merits of incorporating global, industry-led cybersecurity standards into federal acquisition planning and contract administration. The ICT industry is deeply committed to improving cybersecurity and, as such, we are deeply involved in this work and want to make it a success.
- Ensuring private sector participation in the supply-chain work within the Executive branch. As with any cybersecurity issue, public-private partnerships are critical. Currently there are various supply-chain efforts within the Administration. Although it has been challenging at times for the private sector to have input into that work, now both the IT Sector Coordinating Council and Communications Sector Coordinating Council have active supply-chain committees that are working closely with DHS and other government agencies to jointly review this work.
- Sourcing technology from authorized sellers and resellers. Federal purchasers and their contractors should procure ICT equipment directly from original equipment manufacturers (OEMs) or their authorized resellers and service partners, except when the item is discontinued or otherwise unavailable. This can help to minimize the chances that counterfeit or tainted products will be unintentionally acquired, mitigating a significant risk to government supply chain. Too often, we have seen government agencies procure technology products from companies that had no relationship with the products manufacturers, and had themselves bought the products from unverified sellers.
- Passing effective cyber threat information-sharing legislation.

I want to highlight this last point. There is a very important role the government can play in partnership with industry. Effective sharing of actionable information among and between the public and private sectors about cyber threats and incidents is an essential component of improving cybersecurity—including in ICT supply chains. We know from experience that once effectively informed of the specific threats they face, organizations take appropriate and reasonable measures to mitigate them. The Executive Order intends to improve the government's sharing of actionable information with the private sector on specific, targeted cyber threats and technical indicators that flag risks generally. We hope these changes are executed quickly but we also believe Congress can build on the EO by addressing liability concerns that impede information flows. That is why ITI supports the Cybersecurity Intelligence Sharing and Protection Act, which received strong, bipartisan support in the House a few weeks ago. We are working with legislators to continue to improve this bill. We support Senate efforts to adopt a corresponding bill and will push this legislation towards enactment in this Congress.

Government efforts should also preserve the ability of our members' private sector customers, including the telecommunications industry, to leverage our members' compliance with global industry-led standards and best practices. The government has long recognized that taking a light touch approach to regulating the telecommunications industry has fostered innovation and competition, to the benefit of the American consumer. The results are clear. The U.S. now leads the world in fourth generation long-term evolution (4G LTE) deployment, with as many subscribers in this country as there are throughout the rest of the world. In terms of wired broadband, today 80 percent of U.S. households have access to networks capable of 100 megabit speeds. And all the while, the communications industry has been consistently cited as one of the leading sectors in cybersecurity. We encourage Congress to continue this light-touch approach when looking at the communications supply chain and thereby, to enable industry to respond to evolving threats with innovation, flexibility, and the most updated and appropriate global standards and best practices.

Conclusion

Members of the subcommittee, ITI and our member companies are pleased you are looking at how we can improve supply-chain security. As I said at the opening of my testimony, supply-chain security is absolutely critical to our members' success. The protection of our customers here and around the world, our brands, and our intellectual property are essential components of our business and our ability to grow and innovate in the future. We stand ready to provide you any additional input and assistance in our collaborative efforts to develop balanced policy approaches that mitigate risks and ensure the integrity of ICT supply chains. Thank you.