Securing the Network: Cybersecurity Recommendations for Critical Infrastructure and the Global Supply Chain

Telecommunications Industry Association

EXECUTIVE SUMMARY:

The increased integration of information and communications technology (ICT) into the daily activities of industries, governments, families and consumers – along with the corresponding growth of cyberspace – has been a major driver of economic growth and productivity. But just as cyberspace has created unprecedented opportunities for economic growth, it has also created unprecedented opportunities for bad actors. Indeed, the White House has described cybersecurity as "one of the most serious economic and national security challenges we face as a nation."[1] How effectively industry and government work together toward the common goal of securing cyberspace will ultimately impact how secure we will be and the degree to which society continues to reap the benefits of living in the digital age.

Two areas of specific concern include protecting the nation's critical infrastructure (approximately 80-90% of which is privately owned) against cyber threats, along with addressing potential vulnerabilities in the global nature of the ICT supply chain. Both the ICT industry and policymakers share the common goal of addressing these concerns. Regarding critical infrastructure, the current voluntary public-private partnership model has provided private-sector owners and operators with the flexibility they need to address attacks as they occur – particularly as cyber attacks have increased in both volume and sophistication. Significant investments in security from both operators and ICT vendors, strong network management, implementation of best practices and techniques, and voluntary coordination are all essential components of the current ecosystem that has protected critical infrastructure from significant attacks. These components should continue to provide the foundation for critical infrastructure policy moving forward.

In contrast, a mandatory regulatory regime for critical infrastructure would not serve the nation's cybersecurity needs well. But unlike typical policy debates regarding the merits of prescriptive regulations, industry's primary concern with transitioning to a mandatory regulatory regime is not about the misallocation of resources to compliance purposes, or even that compliance efforts would be duplicative of existing activities. Although those concerns are real, the primary concern is that imposing rigid regulatory requirements – requirements that by their nature will be unable to keep up with rapidly evolving technologies and threats – would require industry to focus on obsolete security requirements rather than facing the actual threat at hand, effectively making systems *less* secure. Instead, the key to improving the cybersecurity of critical infrastructure is to strengthen the broader cyber ecosystem that enables rapid information sharing, enhances public private partnerships, and provides sufficient investment to address current and emerging threats.

Meanwhile, the ICT industry is global in nature. The global market and global supply chain for ICT products and services are inexorably linked, with security efforts requiring a global approach based on industry-driven adoption of best practices and global standards. Industry recognizes the weight of policymakers' supply chain concerns, and is equally interested in preserving the security and integrity of its supply chain. Indeed, industry already has a very strong market-based incentive to ensure that networks are safe, reliable, and secure, with industry participants working in partnerships with government entities and even with competitors.

TIA makes the following recommendations regarding how policymakers can provide the owners and operators of critical infrastructure systems with the flexibility they need to address cyber threats as they evolve, along with recommendations for addressing ICT supply chain concerns.

- **Recommendation 1: Efforts to improve cybersecurity should leverage public-private partnerships as an effective tool for collaboration on addressing current and emerging threats.**
- **Recommendation 2: The U.S. government should enable and stimulate greater cyber threat information sharing between the public and private sector.**
- **Recommendation 3: Policymakers and regulators should address economic barriers for owners and operators of critical infrastructure to secure cyberspace.**
- **Recommendation 4: Congress should prioritize federal research funding for ICT and specifically cybersecurity research and development.**
- **Recommendation 5: A global industry necessarily requires a global approach to address cybersecurity concerns.**
- **Recommendation 6: A global supply chain can only be secured through industry-driven adoption of best practices and global standards.**

I. INTRODUCTION

Cyberspace is becoming increasingly integrated and essential to every individual, family, business and government. Since the internet became widely available in 1994, cyberspace has rapidly grown and evolved while dramatically changing entire sectors of the economy. Today, cyberspace generates far-reaching benefits from our largest critical infrastructures to each individual citizen. However, both the amount and value of activity in cyberspace has also created new opportunities for bad actors. As a result, cybersecurity's scope and potential impact on national security and the overall U.S. and global economy continues to increase.

Protecting cyberspace is critical from the perspective of both industry and government. Industry and government share common interests in building confidence and security in the use of information and communication technology (ICT) to promote economic growth and national security. Market forces push ICT firms to place a high priority on the cybersecurity of their products and services. As cyber attacks continue to increase in volume and sophistication, it is critical that the public and private sectors partner to create an ecosystem with the flexibility to address threats as they evolve.

Industry and government both have important roles in the effort to secure cyberspace without diminishing the benefits that it provides. The private sector owns 80-90% of the nation's critical infrastructure and has primary responsibility to secure their networks. Government intelligence identifying threats can help industry protect critical infrastructure along with participation in other public-private partnerships. However, the rapidly-changing nature of cyberthreats means that a mandatory compliance-driven regulatory model would be ineffective and counterproductive in keeping pace. Instead, successful efforts must leverage the fact that the private sector is highly motivated and engaged in addressing both cybersecurity for critical infrastructure and the global supply chain.

II. CRITICAL INFRASTRUCTURE

As with other facets of the U.S. economy, critical infrastructures in the U.S. such as the electric grid, water supply, transportation, financial systems and emergency services have benefitted significantly from greater integration of ICT to make systems more efficient, resilient and reliable. Because of these benefits, it has

become nearly ubiquitous to overlay critical infrastructure assets with industrial control systems and advanced communications systems.

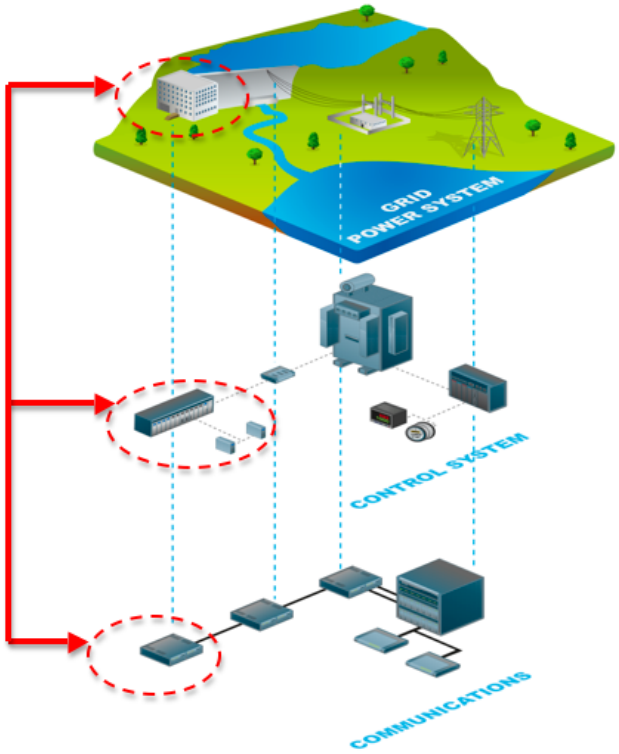


Figure 1: Department of Energy, PNNL, Technology Security Assessment for Capabilities and Applicability in Energy Sector Industrial Control Systems.

The ongoing modernization of the electric grid, as one example, has had and will continue to have far-reaching benefits including: enabling the integration of intermittent energy from solar and wind sources into the grid, enabling the integration of electric vehicles, making possible distributed generation and reducing line loss among a host of other benefits.[2]

The concern shared by both industry and policymakers is the need to secure our ICT-enabled critical infrastructure and accompanying industrial control systems from cyber attacks. While the U.S. has yet to experience a significant breach of critical infrastructure, all signs suggest that critical infrastructure will continue to be subject to an increasing number of attacks. For example, the most recent Incident Response Summary Report from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reported a 400% increase in reported and identified incidents impacting organizations that own and operate control systems associated with critical infrastructure from 2010 to 2011.[3]

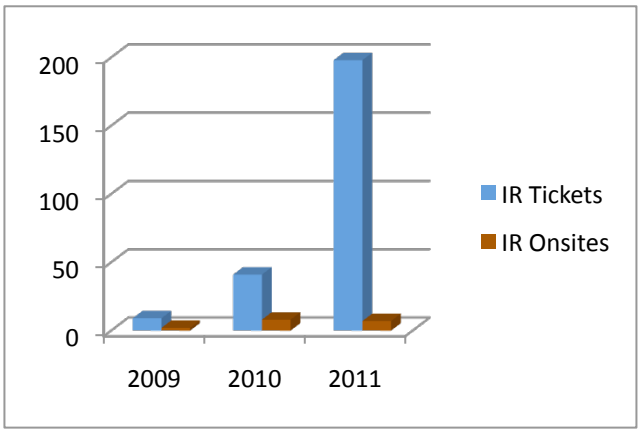


Figure 2: ICS-CERT, ICS-CERT Incident Response Summary Report 2009-2011

In addition to the increasing volume of attacks, industry is also concerned that cyber attacks are growing increasingly sophisticated. Advanced Persistent Threat (APT) attacks have significantly changed the cyber threat landscape by introducing an adversary, likely backed by nation-states, with a high likelihood of success. With a high level of expertise, funding and organization, APT attackers will likely succeed in breaching a targeted system. APT attacks will not be defeated through mandated federal standards, best practices or traditional perimeters. Rather, combating APT attacks will require increased and more rapid information sharing as well as providing the owners and operators of critical infrastructure the flexibility to focus on the attacks at hand. It is impossible to stop all attacks, but it is possible for the government to allow industry the flexibility and agility required to address them.

Owners and operators of critical infrastructure and the private sector more broadly have taken cybersecurity seriously and continually work together sharing information and best practices. The good news is that even though U.S. critical infrastructure is constantly and increasingly attacked, we have not yet seen a major successful breach that has led to serious consequences. The private sector has been successful in thwarting many cyber attacks because the current ecosystem based on voluntary partnerships has allowed industry the flexibility to focus on protecting ICT systems from attack rather than going through a box-checking exercise. Significant investments in security from both operators and vendors, strong network management, implementation of best practices and techniques, and voluntary coordination are all critical components of the ecosystem that has protected critical infrastructure from attacks.

Industry's primary concern with a mandatory regulatory regime is not the resources it would require misallocating to compliance rather than security, or that minimum security requirements would be duplicative of activities they are already doing. The primary concern is that imposing rigid regulatory requirements that by their nature will be unable to keep up with rapidly evolving technologies will require industry to focus on meeting obsolete security requirements rather than the actual threat at hand, which will in effect make critical infrastructures and the customers that they serve less secure. The key to enabling cybersecurity for critical infrastructures is to strengthen the cyber ecosystem that enables rapid information sharing, enhances public private partnerships, and provides sufficient economic resources.

TIA makes the following recommendations that will provide the flexibility needed by the private sector to address cyber threats to critical infrastructure.

- **Recommendation 1: Efforts to improve cybersecurity should leverage and enhance existing public-private partnerships as effective tools for collaboration on addressing current and emerging threats.**

Public-private partnerships have been identified as the foundation for the cyber defense of critical infrastructure and cybersecurity policy for the last decade.[4] Indeed, the success of critical infrastructure owners and operators in repelling increasingly sophisticated attacks has resulted from the voluntary, public-private model – a model capable of evolving along with changes to the critical infrastructure and the risk environment. As both the sophistication and number of attacks increase, it will be critical to leverage and enhance existing public-private partnerships. Transitioning from the successful public-private partnership model to a mandatory regulatory regime would have a negative impact on the security of critical infrastructure.

The National Infrastructure Protection Plan (NIPP), which has formalized the public private partnerships in the 18 critical infrastructure sectors with Sector Specific Plans and Sector Coordinating Councils (SCCs) describes the benefits of the public-private partnership as follows:

> The multidimensional public-private sector partnership is the key to success in this inherently complex mission area. *** [It] has facilitated closer cooperation and a trusted relationship in and across the 18 CIKR sectors. *** Integrating multi-jurisdictional and multi-sector authorities, capabilities, and resources in a unified but flexible approach that can also be tailored to specific sector and regional risk landscapes and operating environments is the path to successfully enhancing our Nation's CIKR protection.
>
> Implementation of the NIPP is coordinated among CIKR partners to ensure that it does not result in the creation of duplicative or costly risk management requirements that offer little enhancement of CIKR protection.

> *** The NIPP provides the framework for the unprecedented cooperation that is needed to develop, implement, and maintain a coordinated national effort to bring together government at all levels, the private sector, nongovernmental organizations, and international partners.[5]

In short, the public-private partnership model for cybersecurity accomplishes what a mandatory model cannot: 1) cooperation instead of compliance, 2) a flexible and unified approach to address attacks, and 3) avoidance of duplicative and costly requirements, thus allowing resources to be focused on protection rather than obsolete mandates.

Between the NIPP and other programs, there are a multitude of public-private partnerships that can be used and enhanced to protect critical infrastructure including the National Coordination Center / Communications Information Sharing and Analysis Center (NCS / ISAC), the National Cybersecurity and Communications Integration Center (NCCIC), the Partnership for Critical Infrastructure Security (PCIS), the Control Systems Security Program (CSSP), the Communications Coordinating Council, the IT Coordinating Council, the Network Security Information Exchange, the Cross-Sector Cyber Security Working Group (CSCSWG), the Communications Security, Reliability, and Interoperability Council (CSRIC), and the NSTAC. While public-private partnerships do not operate perfectly, they should serve as the foundation for moving forward with critical infrastructure protection.

Rather than focusing efforts on a new regulatory regime, TIA recommends that the federal government devote resources to enhancing public-private partnerships as they have proven effective tools in providing industry with the flexibility they need to thwart attacks.

- **Recommendation 2: The U.S. government should enable and stimulate greater cyber threat information sharing between the public and private sector.**

Enhanced information sharing is key to enabling the owners and operators of critical infrastructure to address cyber threats. The government should provide more timely and detailed cyber intelligence to industry to help identify threats to private networks. The GAO has found repeatedly that the expectations of private sector stakeholders regarding the sharing of cyber threat information are not being met, and has recommended enhancing information sharing efforts.[6]

The government is also in a position to significantly enhance the ability of private sector participants to share cyber threat information among themselves and with the government. Current legislation that has already passed the House with broad bipartisan support, the Cyber Intelligence Sharing and Protection Act, would make significant strides towards reaching this goal. Industry has proven motivated and capable of strong cooperation to combat cyber threats and is waiting on Congress to remove barriers to more effective collaboration. Additionally, industry will continue to work together to further develop standard, unified methods to collect, analyze and report data breaches at a global level to provide both industry and government with a better understanding of cybersecurity threats.

- **Recommendation 3: Policymakers and regulators should address economic barriers for owners and operators of critical infrastructure to secure cyberspace.**

Increasing evidence suggests that economic considerations are a significant factor for owners and operators of critical infrastructure protecting their networks. As the Cyberspace Policy Review commissioned by the White House noted, "[m]any technical and network management solutions that would greatly enhance security already exist in the market place but are not always used because of cost or complexity."[7] For industries currently operating under a regulatory

regime, their primary regulators need to insure that the owners and operators of critical infrastructure are provided sufficient investment to address cyber threats. For less-regulated industries, policymakers can supply economic incentives by using liability reforms, which decrease the potential costs of sharing information.

The Cyber Intelligence Sharing and Protection Act passed by the House will help remove some of these economic barriers. Ultimately, ensuring that owners and operators have the financial resources to acquire and maintain adequate security systems – systems that already exist in the market – will be significantly more effective in protecting critical infrastructure than mandating requirements.

- **Recommendation 4: Congress should prioritize federal research funding for ICT and specifically cybersecurity research and development.**

While the U.S. still boasts the strongest research ecosystem in the world, there are signs of erosion in the ICT sector as competing nations take strong steps to attract investment in ICT research to build innovation-based economies.[8] The consequences for the U.S. ICT sector of a less competitive ICT research ecosystem are very real. As the National Academy of Sciences observed, "[t]he nation risks ceding IT leadership to other generations within a generation unless the United States recommits itself to providing the resources needed to fuel U.S. IT innovation."[9] Yet the U.S. government has not made a strong enough commitment to prevent this forecast from becoming a reality – federal investment in ICT research remains relatively low compared to other scientific fields. Beyond the economic costs of other nations surpassing the U.S. in ICT research, the most alarming costs are in the implications for national security.

Congress should prioritize federal funding for cybersecurity research and development, and should coordinate research activities between different participating agencies with industry input. Congress should also facilitate greater private investment in research more generally through the enactment of a permanent, simplified, R&D tax credit.

SUPPLY CHAIN

The ICT revolution has been driven by a global environment based on open trade and global market access. This global marketplace has created significant benefits for U.S. industry by opening markets for high-tech U.S. goods and services. Meanwhile, a global ICT supply chain has developed in tandem with the global market.

Policymakers around the globe have begun to express concern about the global nature of the supply chain for fear of hostile actors, abroad or locally, manipulating and sabotaging ICT systems. The Director of National Intelligence, for example, recently identified "the highly complex vulnerabilities associated with the IT supply chain for US networks" as one of the greatest strategic challenges regarding cyberthreats.[10]

Software has been identified as potentially vulnerable. A supply chain attack can be directed at any category of software, including custom software, software delivering a cloud service, a software product, or software embedded in a hardware device.[11] The apprehension with the commercial software development process often revolves around the design and quality of the code. Parties have expressed concern about unprotected portions of code that leave a backdoor open for individuals or governments with adverse interests to subvert the software operation. Moreover, the potential exists for counterfeit software that does not meet a company's standard to be placed in the supply chain and passed off to consumers as the real thing.

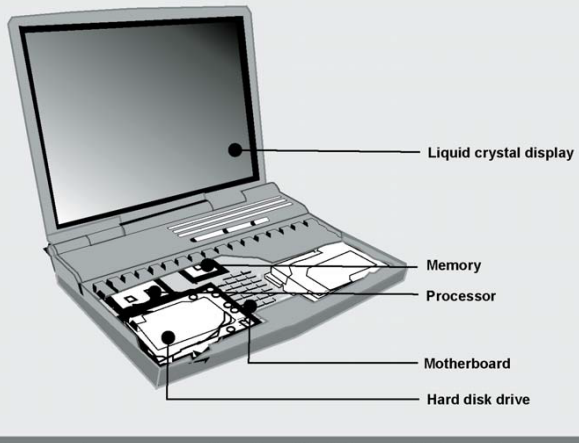
Similarly, there is apprehension about the nature and quality of ICT hardware components. The existence of counterfeit products has also been raised in this context. Risks involving

counterfeit hardware can involve the presence of "fake" products as well as selling or using old parts as if they were new within the supply chain process. [12] Other potential risks include installation of malware, viruses, or other malicious items onto devices in the manufacturing process, leaving devices vulnerable to remote control or corruption once installed in the user's environment.

Industry has proven itself highly motivated to work together to address the issue of hardware and software assurance. TIA makes the following recommendations regarding supply chain security.

- **Recommendation 5: A global industry necessarily requires a global approach to address cybersecurity concerns.**

ICT products are often designed and built in different locations using globally-sourced components, making it very difficult to classify specific products as U.S. or non-U.S. products. For example, a recent GAO study used the following diagram to outline the complexity of the supply chain for a common piece of ICT equipment – the laptop.



Component	Location of facilities potentially used by suppliers
Liquid crystal display	China, Czech Republic, Japan, Poland, Singapore, Slovak Republic, South Korea, Taiwan
Memory	China, Israel, Italy, Japan, Malaysia, Philippines, Puerto Rico, Singapore, South Korea, Taiwan, United States
Processor	Canada, China, Costa Rica, Ireland, Israel, Malaysia, Singapore, United States, Vietnam
Motherboard	Taiwan
Hard disk drive	China, Ireland, Japan, Malaysia, Philippines, Singapore, Thailand, United States

Source: GAO analysis of public information.

Figure 3: GAO Report on Supply Chain Security

Aside from the complexity in defining the nationality of a particular product, ICT companies conduct different functions (manufacturing, R&D and services) across facilities in multiple different countries, often making it difficult to classify companies as U.S. or non-U.S. companies. To stay competitive, ICT companies need to continue to use a distributed approach to their technology development and manufacturing.

TIA strongly agrees with the House Republican Cybersecurity Task Force Recommendations for approaches to address supply chain concerns:

> Any approach must involve international cooperation and heavy engagement with the private sector but should not include language that might put the government in a position to determine the future design and development of technology. Much like the law enforcement provisions, the U.S. must work with other governments to establish

international security standards in order to prevent hobbling U.S. industry with U.S.-only standards. We are concerned about the impact on U.S. global competiveness as well as technology innovation and development of having the U.S. government set specific technical standards.[13]

The U.S. government should not enact 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 cite similar concerns regarding foreign ICT equipment and are currently considering trade restrictive measures. TIA recommends that the U.S. government exercise extreme caution in how it approaches this issue since U.S. policy will effectively serve as a global standard. If the U.S. develops unique approaches that restrict trade unnecessarily, U.S. global economic competitiveness could be severely affected by other export markets adopting similar restrictive policies.

- **Recommendation 6: A global supply chain can only be secured through industry-driven adoption of best practices and global standards.**

The global ICT industry depends on a globally flexible supply chain, characterized by intense competition and fluctuation in price and supply of different inputs. 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. As a result, TIA believes the focus of security concerns should be on how a product is made – not where.

Government entities are concerned about the risks presented by use of parts and components from around the world for the production of high-tech devices being used in the United States. Industry recognizes the weight of policymaker concerns and is equally interested in maintaining the security and integrity of its supply chain, since it has strong market-based incentives to insure that networks are safe, reliable, and secure. 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.

The Open Group Trusted Technology Forum (OTTF) is one of a number of efforts involving the ICT industry that is aimed directly at the supply chain issue. OTTF is a collaborative public-private initiative spearheaded by the Department of Defense and with the other members consisting of representatives from commercial technology companies. The 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.

Furthermore, a group of commercial ICT providers have formed an industry-led effort called SAFECode that is aimed at addressing software product assurance. The organization's mission is to address the concerns about the manufacturing process for ICT products by advancing the use of effective software assurance methods. It is a global, industry-led effort 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.

SAFECode has coordinated with the DHS Software Assurance Forum.

These efforts already being engaged in by industry members utilize the right approach by developing best practices and standards. TIA believes that 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. 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.

IV. CONCLUSION

Owners and operators of critical infrastructure have the primary responsibility for the security of their networks and have proven motivated and effective in addressing increasing and evolving cyberthreats. Moving forward, continuation of a voluntary public-private partnership model will be key to providing the flexibility needed to address threats as they evolve. TIA does not believe that mandated performance requirements will be able to keep pace with a rapidly changing technology and threatscape, thus making a prescriptive regulatory regime unsuitable for addressing cybersecurity concerns. Moreover, industry is committed and engaged in addressing supply chain vulnerabilities from the ground up utilizing voluntary, industry-based standards on a global basis.

When it comes to cybersecurity, industry recognizes that everyone – governments, ICT manufacturers, owners and operators -- are in this fight together, with industry participants setting aside their own competitive interests to solve a problem that concerns all. TIA and our member companies look forward to continued engagement with policymakers as our partners.

[1] White House Comprehensive National Cybersecurity Initiative, available at www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

[2] TIA, *Smart Grid Policy Roadmap* (Feb. 2011) available at www.tiaonline.org/sites/default/files/pages/TIASmartGridPolicyRoadmap.pdf.

[3] ICS-CERT, *ICS-CERT Incident Response Summary Report 2009-2011*, 2 (Jun 2012) available at www.us-cert.gov/control_systems/pdf/ICS-CERT_Incident_Response_Summary_Report_09_11.pdf.

[4] Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, 18 (2009) available at www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf:

[5] National Infrastructure Protection Plan, i-8 (2009) available at www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

[6] GAO, *Testimony Before the Subcommittee on Cybersecurity, infrastructure Protection, and Security Technologies, House Committee on Homeland Security, Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems*, 8 (March 16, 2011).

[7] Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, 31 (2009) available at www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[8] TIA, *U.S. ICT R&D Policy Report*, (2011) available at http://www.tiaonline.org/sites/default/files/pages/TIA%20U%20S%20%20ICT%20RD%20Policy%20Report.pdf.

[9] NRC, *Assessing the Impacts of Changes in the Information Technology R&D Ecosystem: Retaining Leadership in an Increasingly Global Environment*, 1 (2009), available at www.nap.edu/catalog/12174.html.

[10] James Clapper, Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community*, Senate Select Committee on Intelligence Hearing, (Jan. 31, 2012) available at http://intelligence.senate.gov/120131/clapper.pdf.

[11] SAFECode, *The Software Supply Chain Integrity Framework*, (July 21, 2009) available at www.safecode.org/publications/SAFECode_Supply_Chain0709.pdf.

[12] Hearing to Receive Testimony on the Committee's Investigation into Counterfeit Electronic Parts in the Department of Defense Supply Chain, 2 (Nov. 8, 2011) available at http://armed-services.senate.gov/Transcripts/2011/11%20November/11-72%20-%2011-8-11.pdf.

[13] Recommendations of the House Republican Cybersecurity Task Force, 19 (Oct. 2011) available at http://thornberry.house.gov/UploadedFiles/CSTF_Final_Recommendations.pdf.

FOR MORE INFORMATION:
Danielle Coffey, Vice President, Government Affairs, TIA , +1.202.346.3242, email: dcoffey@tiaonline.org

Joseph Andersen, Director, Technology & Innovation Policy, TIA, +1.202.346.3249, email: jandersen@tiaonline.org

Dileep Srihari, Director, Legislative & Government Affairs, TIA +1.202.346.3248 email: dsrihari@tiaonline.org