ARMED FORCES COMMUNICATION AND ELECTRONICS ASSOCIATION
CYBER COMMITTEE

Supply Chain Risk Management Awareness[*]

Jarrellann Filsinger, National Archives and Records Administration
Barbara Fast, CGI
Daniel G. Wolf, Cyber Pack Ventures
James F. X. Payne, Telecordia
Mary Anderson, Booz Allen Hamilton

February 2012

Introduction

Continued globalization marks today's information and communications technology (ICT) marketplace. Mission critical systems and networks extensively leverage commercial, globally interconnected and globally sourced components. These components include hardware, software and firmware and while global sourcing provides innumerable economic and innovative benefits, it also provides our adversaries with increased opportunity to compromise the supply chains of our critical systems. The risk of impeded or compromised components is not unique to US Government systems; it is applicable to commercial vendors in the telecommunications space, and applicable as well to any system regardless of mission. Besides malicious intent, there are a number of factors that drive supply chain counterfeiting and breaches in privacy and intellectual property (protection) that are common across many business sectors, including financial incentives, and short-term performance and profitability. Supply chain risk is a global risk. Formally, supply chain risk is:

> "The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of an item of supply or a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of a system."
>
> *The Ike Skelton National Defense Authorization Act for Fiscal Year 2011, (Section 806).*

This paper on Supply Chain Risk Management (SCRM) is intended to raise awareness of the risks, highlight current issues surrounding supply chain risks, list current initiatives that may further mitigate supply chain risk, and put forth continuing challenges to promote actionable results.

Approach

This paper has the express purpose of raising awareness to an issue of growing concern. As a means of creating a greater understanding of the issue, the AFCEA Cyber Committee formed a subcommittee on Supply Chain Risk Management. The subcommittee is a composition

[*] The views or opinions presented in this paper are solely those of the authors and do not necessarily represent those of the organizations.

of agency and private sector representatives that are close to this issue. As a means of addressing awareness and progress in this area the subcommittee invited a broad range of subject matter experts to discuss the issues in a frank manner. The participants in these interviews were from the highest levels within the government and the private sector. None of the interviewees will be mentioned by name. This was done in an effort to foster candidness and bring forward the important issues that are presently being addressed as well as those issues **not** receiving enough attention.

Scenario

The following compromised supply chain scenario magnifies the extent of the counterfeit threat and the millions of dollars lost to US business and the US Government. Although scenarios like the one below are in the news, awareness of the growing problem is just beginning to surface to a more broad audience.

> "The Justice Department recently (revealed) that Federal authorities over the past five year have seized more than $143m worth of counterfeit Cisco hardware and labels in a coordinated operation that's netted more than 700 seizures and 30 felony convictions.
>
> Operation Network Raider is an enforcement initiative involving the FBI, Immigration and Customs Enforcement and Customs and Border Protection agencies working to crack down on the bogus routers, switches and other networking gear. In addition to costing Cisco and other US businesses millions of dollars, the scams could threaten national security by infusing critical networks with gear that's unreliable or, worse, riddled with backdoors.
>
> As part of the operation, a Saudi citizen residing in Texas, was sentenced this week to 51 months in prison and ordered to pay Cisco $119,400 in restitution after being found guilty of trying to sell counterfeit gear to the US Department of Defense. In 2008, he attempted to traffic 100 gigabit interface converters that were bought in China and contained labels fraudulently indicating they were genuine Cisco equipment, according to court documents. The kit was to be used by the US Marine Corps for communications in Iraq. In another case a Chinese resident in the US was ordered to serve prison time and pay restitution of $790,683 for trafficking counterfeit Cisco gear, officials said.
>
> The prospect that government and business networks may have deployed bogus gear has raised national security concerns, since much of the counterfeit equipment originates in China. Similar espionage fears were raised by University of Illinois researchers, who in 2008 showed how they were able to modify a Sun Microsystems SPARC microprocessor to effectively create a hardwired backdoor capable of logging passwords or other sensitive data. In response, Cisco stated that there was no evidence that any of the counterfeit networking gear contained backdoors.
>
> Since late 2007, US authorities have made more than 1,300 seizures of 5.6 million bogus semiconductors. More than 50 shipments were falsely marked as military or aerospace grade devices."

ChannelRegister.co.uk 7 May 2010

Supply Chain Issues

Research indicates that supply chain issues are numerous and often not well known as a whole. This section summarizes the dominate issues discovered in the research of this topic with government and industry leaders.

*SCRM is a **Global** problem.*

Due to the global nature of supply chain threats, there is a need for recognition and assessment of global interdependencies among purchasers and suppliers. Supply chain integrity and risk mitigations are not intended to target any particular country or specific countries. The current goal is to make our supply chains more safe and secure: "What are the SCRM problems?" and "How to address the problems?" The answers to these basic questions have been in progress for many years and among a variety of organizations without complete resolve. Elevation of supply chain risk to the global arena puts its potential solutions outside the purview of any one organization or government entity.

*SCRM should be an active **Public-Private Partnership** initiative.*

As with other cyber security issues, an effective SCRM approach requires a strong public-private partnership. Within the government, there are multiple agencies with SCRM interests and authorities; similarly, industry interests and needs are varied and differ by sector. There are clear authorities for the government to assume the leading role in law, policy, and standards. However, the private sector can play a key role in a number of areas.

A public-private partnership that consists of voluntary adherence vice prescribed law or regulation is viewed as leading to a more positive outcome. Keys to success are dialogue, incentives, voluntary risk assessments, and information sharing (both public and private).

Information sharing today between the public and private sectors is growing, but still inconsistent. Government agencies share amongst their organizations, there are industry-to-industry partnerships, and there is some level of public-private sharing between government and industry. The latter is hampered by concerns over Freedom of Information Act, lack of safe harbors, and liability. Minimum information sharing areas include best practices, risk assessments, incident reporting, and solutions. Ideally, a framework and process for sharing would greatly facilitate the multiple approaches being used today. For public-private partnerships, a goal for information sharing should include best practices, risk assessment methodologies and anonymized results, incident reporting, and solutions. The public-private partnerships are sharing some of information, but these exchanges of critical information are inconsistent and very dependent on organizational and/or personal relationships. There are examples of efforts to raise awareness for supply chain integrity throughout the government, but there is no government-wide initiative to address change, mitigation, or resolution. The

Comprehensive National Cybersecurity Initiative on Supply Chain Risk Management (CNCI-SCRM) goes the furthest, thus far. Legislation under current consideration titled the Promoting and Enhancing Cybersecurity and Information-sharing Effectiveness[1] (PrECISE Act) include proposed provisions to encourage sharing, but falls short of mandating the exchange for sectors identified as critical to national security. Provisions in the proposed bill would mandate Department of Homeland Security (DHS) to evaluate cybersecurity risks in the critical infrastructure and to determine appropriate mitigation strategies.

Federal policy and regulation only goes so far. The Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation (DFAR) only apply to federal procurement and not to state or private systems. Even the FAR/DFAR are limited, dealing with acquisition that does not address operational and security aspects of the procurement.

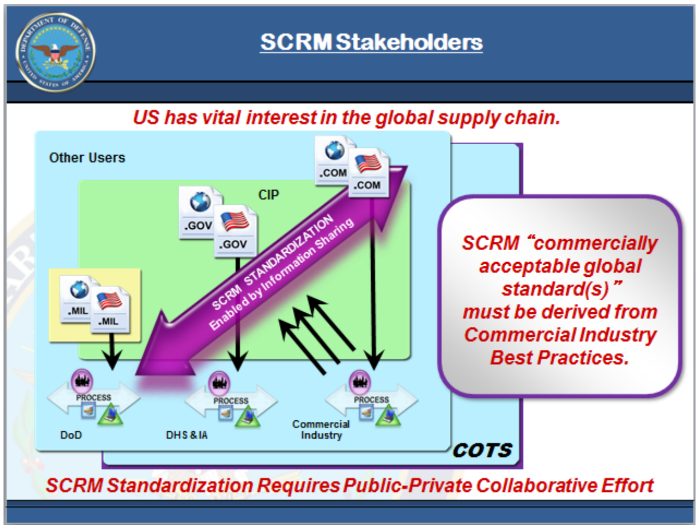
Industry practitioners of SCRM have a different view of the problem, especially the risk factors. As companies, their brand is their business. Many industries have processes in place to check for counterfeit or malicious materials and some of these are good candidates as ‘best practices’. For example, the Trusted Technology Forum under the Open Group is developing a process like Common Criteria that certifies companies based on factors such as: standards, processes, assurance and integrity. In some ways, the industry approach complement the government initiatives. Working closer together might result in a more comprehensive public-private solution.

Incentives that provide assistance to foster technology innovations is a public-private sector partnership to address supply chain risk. Assistance by the government to enable American technology providers would help secure their future as part of a cyber security umbrella. Plans that span from idea incubation to capability maturity could create a decided advantage for SCRM.

Figure 1[2] SCRM Stakeholders shows a cross section of government and industry working towards SCRM standards based on commercial best practices.

[1] H.R. 3674 will amend the Homeland Security Act of 2002 to make certain improvements in the laws relating to cybersecurity, and for other purposes as introduced.

[2] “Our Globalized Supply Chain”. Don Davidson. Trusted Mission Systems and Networks (TMSN) /DoD CIO.



SCRM Stakeholders

US has vital interest in the global supply chain.

SCRM "commercially acceptable global standard(s)" must be derived from Commercial Industry Best Practices.

SCRM Standardization Requires Public-Private Collaborative Effort

Figure 1: SCRM Stakeholders

*We need to know the full spectrum of the SCRM **Risk**.*

Supply chain risk stems from multiple factors: growth in dependencies on foreign technology, infrastructure risks, inadequate procurement practices, and deficient standards.

As a consequence to the US pursuing an outsourcing strategy during the last few decades, the US has begun to lose its leadership in many technology areas. The risk is that the US is very dependent on foreign sources for our hardware, firmware and software. This makes understanding our risks and better securing the supply chain a critical goal, especially when most of our sources of technology are overseas. In general switching back to only American hardware and software is impractical, expensive, and impossible with the exception of highly sensitive specialized components already addressed by the Trusted Foundry program.

Meanwhile our acquisition processes have not adequately addressed the threat of malicious intentions within foreign or US produced products. The US has not implemented rigorous acquisition security practices to enable detection of inferior components. The US needs to improve robustness in its acquisition processes to include models to evaluate risk associated with specific decisions in a system life-cycle. These life-cycle processes should include software and system integrity and assurance requirements that will provide purchasers the insight into the processes under which the product was developed.

At the same time, improving security standards maybe at risk; as foreign entities are becoming more involved in the various worldwide standards bodies. As a result there is an increased risk of specification of weak or ineffective security standards either through unintentional technical weaknesses or through malicious intent. The US should reemphasize the importance of global standards and reengage in standards development organizations to ensure rigorous evaluation of specifications. Good standards reduce risks in the supply chain. A goal of the current Administration is to embrace and advance global standards and to encourage collaboration with other stakeholders seeking to contribute to this collective mission.

The US telecom industry is a critical component of the US critical infrastructure. The risk is the lack of detailed knowledge of the specific threat and poor definition of potential solutions. Along with telecom, energy, and the financial sectors are special categories because of the high payoff from an incident it offers to an attacker. These three sectors of the critical infrastructure/key resources are the backbone of all the other critical sectors in the infrastructure. In recent international forums working treaty issues, representatives have discussed cybersecurity and potentially horrendous hacking attacks on critical infrastructure components where serious collateral damage could have life threatening effects on the civilian population or financial impacts on the world economy. For example, the international members have considered the impact of attacks on the power grid, financial networks, or water supply infrastructure and compared these to chemical/biological weapons attacks. As a result, the negotiators are considering international cyber security treaties to ban certain types of cyber attacks on the critical infrastructure.

There is a lack of metrics to characterize the supply chain problem. Without a giving the problem some dimension, the risk cannot be quantified or measurably improved. There are only sketchy metrics about incidents within the supply chain. Various scoring procedures already exist. Several Intelligence Community acquisition security organizations are using scoring procedures to do a risk evaluation. Mission elements or acquisition organizations can then use this data to assess risk and make contracting decisions. The PrECISE Act is proposing that DHS work with industry practitioners and other government organizations to evaluate these existing processes and adopt the "best in class" as part of the common risk assessment process.

Today, liability issues tend to restrict sharing of metrics information. Divulging vulnerabilities or reporting an incident can have a negative reaction from the stockholders and can provide an unfair advantage to a competitor. Once these liability issues are minimized, sharing of metrics should become a priority to keep all acquisition authorities informed.

When one evaluates risk in the supply chain, it is important to look at multiple factors, which include determining the actual threat, identifying the vulnerabilities in our systems, calculating the capabilities of our adversaries, determining the intentions of malicious actors, and evaluating the actual cost/impact of compromised component. Along with these, it's important to develop models and to gather metrics to evaluate and prevent incidents. To reduce supply chain risks, a well-defined lifecycle processes that evaluates threats and vulnerabilities coupled with adversarial intentions and capabilities. Given these factors, risk models will enable evaluation of supply chain risk mitigation strategies.

***Cultural** shifts are considered necessary to address SCRM.*

SCRM is a global issue complicated by corporate liability and market forces. In the US, the elements of democracy vis-a-vis governmental checks and balances; leads to seemingly fragmented decision making and addressing SCRM issues more difficult. To work within these challenges, it is imperative to acknowledge that as whole, *we live in a bad neighborhood*. In place of the current piecemeal method, a new business paradigm encompassing a systematic approach is required along with recognition that not all countries share the same set of economic values and business models. At present, existing US policy on SCRM focuses on discrete aspects of the SCRM issue without tackling the larger pervasive problem. The future of SCRM needs to move from just "protection" to a more inclusive culture of "assumption of vulnerability."

This concept of "assumption of vulnerability" is wholly ignored in the competing marketplace where product price sensitivity is vital. If an item is priced 50% less from competing products a buyer is more likely to purchase the lesser priced item. However, this purchasing decision needs to question not only why an item is 50% cheaper than competing products but also: How is it produced? Where is it from? Which software programming language was it implemented with? What vulnerabilities might I be accepting when I buy the cheaper product?) This "assumption of vulnerability" concept will help the fight against counterfeit products and validate the need for a product's pedigree which will reflect its make-up and authenticity. The surprising issue is that, in many cases, there are many similarities between counterfeit products and their authentic sources; thereby making it extremely difficult to determine when a component is counterfeit.

If this cultural pivot fails to take place, SCRM will continually be in a reactive mode. Addressing these crucial vulnerabilities is a daunting but imperative task; however, becoming overly protective to the point of insulation defeats the construct of the global supply chain. With the increased focus on technology, the future of SCRM needs to focus on a manageable containment strategy that can continue to function in a changing market economy.

***Current Efforts** on SCRM are not sufficiently focused.*

SCRM work being done across the US government lacks focus and a prioritization is needed for more effective mitigation of this complex and threatening problem. This paper documents the many initiatives but there is a repeated call for more attention and coordination between and among the public and private sectors. The list of current efforts by some standards could be considered impressive, however, there is no consensus on the definition, scope or mitigation plan to this problem. Without an agreed scope of the problem, it appears as if we are talking past each other. The central debate is around the appropriate role of government. Should this problem be resolved by fiat meaning the development of trusted vendor lists or a thorough reform of the government procurement process? Or is the needed approach a call for a common risk assessment methodology and related process? The latter approach requires the needed public-private dialogue. Using this common risk assessment approach allows market forces to intervene and work toward a resolution. Parties tend to align politically along these lines. It is probably a combination of both approaches. For certain the government needs to understand the full implication of the regulations should they decide to take this route. There are many interdependencies that exist in the public sector and simple changes to the FAR/DFAR can have unintended consequences. It is clear that there is no distinguishing between American manufactured and foreign sourced equipment. We all appear to be using similar sources and benefiting from cheap labor and less restrictive manufacturing regulatory practices across the globe. This adds to the complexity and therefore does not offer a simple solution. Other countries appear to be making progress by working the issues through legislation and looking to partner with the private sector. The objective is to create a better global supply chain process, **not** eliminate the global supply chain or limit access, to only acceptable countries.

Telecommunications is a critical sector and is uniquely vulnerable to SCRM and therefore necessitates a call for more awareness about this sector and an increase in public/private sector dialogue as the correct means of mitigating this problem. It has been pointed out that the first serious look at this problem has its roots in a classified initiative in 2004. Not much progress has been made in the intervening years and yet this problem looms on our horizon even larger now eight years later. Current methods of interaction are not resulting in a meaningful dialogue in the timeframes needed.

SCRM ***Standards*** *reduce risks.*

There is a debate on whether standards should be mandatory or voluntary, but there is little disagreement on the need for standards, global standards. Work on standards includes a variety of areas, to include procurement, software assurance, risk methodology, etc. There is some advocacy for high value/critical sectors requiring suppliers to meet standards that would be prescribed. Ideally, some level of standards is viewed as beneficial to all government and industry procurements due to the nature of the threat. Voluntary adherence to standards could be more popular if there were incentives for meeting minimum thresholds. There is also a debate on whether a voluntary set of guidelines should be implemented to prevent mandatory provisions—and to speed along recognition of the need before a catastrophic event might occur.

A number of organizations have published guidance or some subset of SCRM standards, to include National Bureau of Standards and Technology, International Standards Organization, and American National Standards Institute. Many of these efforts have included international participation which facilitates international adherence to this global problem. The international nature of these efforts, while deemed positive, also has created a "politicization" that has second order implications. There are often limited filters placed on joining a standards development effort. Participants can range from highly skilled and technical to those who essentially "apply or buy their way in." The agenda of some participants vary from the pure hearted sense of national/international security duty to a profit motivated interest or even malicious intent. Not all participants of standards initiatives share our national interests; indeed, some would say that the foxes are already in the hen house. By working “within the system” these learning and adaptive potential adversaries gain an advantage in understanding our strengths and weaknesses. Therefore, while a standards development process serves to strengthen SCRM, it also may create unintended consequences. All the more reason, some would say, for a basic philosophy that we should accept that our supply chain is vulnerable and that we need to accept and manage the risk.

Supply chain risk mitigation standards are moving into the engineering of the product, rather than just an inspection of the product. When accepting that the risk not avoidable, the focus of mitigation from an engineering point of view becomes: How can I mitigate the risk of a faulty or compromised component? More of the SCRM standards initiatives are software assurance in nature, concentrating on ensuring that integrity of the component is built into the product.

Current Initiatives

Supply chain best practices and current initiatives have been in development since the early 1980’s. However, the supply chain threat is now recognized as a major cyber threat affecting development and operation of computer systems and not just a threat to the transportation of material and goods from supplier to purchaser. Annex A contains a wide selection of the best practices and current initiatives on supply chain risk management.

Continuing Challenges

Many of the current approaches to mitigating supply chain risks pertain to software or hardware engineering integrity and assurances; are we willing to accept the additional costs associated with these engineering practices?

What is the solution for national and international standards development organizations that have membership by companies that intend to influence standards to the detriment of safe computing, thus undermining effective supply chain risk management practices?

What types of incentives are needed to encourage private industry to partner with the government to optimize the protection of the supply chain?

How can we better sensitize the law makers to the reluctance and significant restrictions on public- private dialogue where admission of known vulnerabilities can lead to onerous liability lawsuits against corporations and their officers?

Summary

While we recognize that supply chain risk has grown from multiple factors: dependencies on foreign technology, infrastructure vulnerabilities, inadequate procurement practices, and deficient (product integrity) standards, it is now necessary to converge efforts on managing risk as opposed to eliminating risk, as the latter is not possible; our focus should be on eliminating risk, where possible, but managing acceptable risk to our most critical systems and better provide high quality products and services where absolutely needed. This concept is truly a risk based approach to the problems faced when globally outsourcing. Supply chain risk cannot be delegated to a single sector to resolve, it has to be recognized as a global issue requiring a multi-cultural, multidisciplinary approach to include standards, engineering, technology, legal and procurement specialists all with the similar intent.

Awareness of supply chain risks throughout a systems life-cycle is an all important objective for mitigating compromised components. People at all levels within an organizations hierarchy should recognize supply chain risk. Identification of who and what is within an organizations supply chain is critical for gaining visibility into what is happening within it , as well an monitoring and indentifying adverse events. Without this due diligence, supply chain compromises will continue to escalate unbounded.

The solution set for managing supply chain risk cannot be a one-size – fits all resolution. To some extent costs for minimizing risks will weigh differently depending on the product and the sector in which it will be deployed. Potential supply chain risks can be mitigated by including rigorous security engineering and review processes in our software/hardware development, but at a price not conducive for everyday products. Rather, the high assurance engineering of supply chain risks are applied to critical system components. In time, the engineering of integrity into system components will become a standard operating practice and cost saving will follow.

Incentives to propel the public-private partnerships are vital for discussing and resolving supply chain risk management. This action on the part of Government may lead to working through liability, incident sharing, and proprietary issues that seem to block progress toward open acknowledgement of our growing supply chain problem.

Annex A

Supply Chain Best Practices and Current Initiatives

Supply Chain Risk Management, Information Technology Laboratory, NIST. Web site created Nov 2009; updated July 2011. http://scrm.nist.gov The NIST web site describes a NIST project to create toolset of supply chain assurance methods and techniques for industry and government. It contains an extensive knowledge base of SCRM articles, and best practices.

Common Criteria: Embrace, Reform, Extend. Intel Corporation and CISCO. Discussion Draft 1.0. June 2011.The document discusses requirements for assessing the security assurance of ICT products use a process that provides internationally harmonized evaluations standards and promotes efficiency and reasonable value.

Common Criteria Reforms: Better Security Products through Increased Cooperation with Industry. NIAP/CSS Commercial Solution Center (NCSC), Chris Salter, January 2011.This document explains the motivation of the Common Criteria reforms underway. The Common Criteria Development Board (CCDB) is considering the stand-up of a new Supply Chain Technical Working Group to advise new/emerging Common Criteria Protection Profiles.

***Draft* NISTIR 7622, *Piloting Supply Chain Risk Management for Federal* Information *Systems*, June 2010.** This document provides a set of practices that can be used for those information systems categorized at the FIPS (Federal Information Processing Standards) 199 high-impact level. These practices are intended to promote the acquisition, development, and operation of information systems or system-of-systems to meet cost, schedule, and performance requirements in today's environment with globalized suppliers and active adversaries. Integrated within the information systems development life cycle (SDLC), these practices provide risk mitigating strategies for the acquiring federal agency to implement.

Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain, June 2010. SAFECode. SAFECode addresses the emerging area of software integrity which is one of engineering practices contributing to software assurance. The document addresses sourcing, development and delivery integrity controls for mitigating supply chain risk.

Evaluating and Mitigating Software Supply Chain Security Risks, May, 2010, Carnegie Mellon/ Software Engineering Institute. The report provides an assurance case reference model showing how gathered evidence is combined into an argument demonstrating that supply chain security risks have been addressed adequately throughout the acquisition life-cycle.

The **US-CERT** maintains the **Software Assurance (SwA) Pocket Guide Series** on software assurance in acquisition and outsourcing, system development, system life-cycle, and measurement. SwA Pocket Guides are developed collaboratively by the SwA Forum and Working Groups which function as a stakeholder community that welcomes additional participation in advancing and refining software security. The SwA Pocket Guide Series can be found on https://buildsecurityin.us-cert.gov/swa/pocket_guide_series.html.

Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11: Supply Chain Risk Management Pilot Program. February 25, 2010. (https://diacap.iaportal.navy.mil/pages/scrm.aspx)

Trusted Integrated Circuits (IC) Suppliers available from http://www.dmea.osd.mil

SCRM assistance and references from the Department of Homeland Security, Global Cyber Security Office can be found by contacting DHS_SCRM@dhs.gov. Agencies may contact Software.Assurance@dhs.gov for assistance in the development of a software assurance capability.

Selected **SCRM industry standards** listed below pertain to quality assurance for electronic components.

a. EIA-4899 - Standard for Preparing an Electronic Component Management Plan
b. IDEA-STD-1010 – Diminishing Manufacturing Sources and Material Shortages (DMSMS) Guidebook
c. SAE-AS9120 – Quality Management Systems for Aerospace Product Distributors
d. SAE-AS5553 – Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition

The Open Group's Trusted Technology Forum (OTTF) has recently developed a (draft) snapshot/framework to address anti-counterfeiting and anti-tainted product. (Press Release 6 Mar 2012). See www.opengroup.org.

International Standards Organization published the ISO 28000 series of standards to facilitate safe trade and transportation of goods. **DRAFT ISO/IEC 27036:** Information Technology – Security techniques –Information Security for Supplier Relationships. **ISO/IEC 15026** System and Software Engineering – Systems and Software Assurance – Part 2 Assurance Case.

National Defense Industrial Association (NDIA) System Assurance Committee, 2008. *Engineering for System Assurance*, Arlington, VA. This document provides guidance on how to build assurance into a system throughout its life cycle. It identifies and discusses system engineering activities, process, tools and considerations to address system assurance. Assurance guidance used by the DoD and its contractors is also included in the document.

National Strategy for Global Supply Chain Security, Office of the Press Secretary, the White House, January 2012. www.whitehouse.gov. The strategy includes two goals: To promote the efficient and secure movement of goods, and to foster a resilient supply chain.