Defense Supply Chain Security:

Current State and Opportunities for Improvement

By:
Jacques S. Gansler, William Lucyshyn,
and Lisa H. Harrington

Center for Public Policy and Private Enterprise

School of Public Policy

December 2012
This research was partially sponsored by a grant from Lockheed Martin Corporation

University of Maryland 18 56

Table of Contents

Table of Contents ii
Table of Figures iii
Executive Summary iv
Security Concerns on the Rise iv
What this Report Covers v
Introduction & Focus 1
I. Overview: Supply Chain Security and DoD 3
Definition of Supply Chain Security 3
Why Security Risk is Increasing 7
II. DoD's Supply Chain Vulnerabilities 10
The Problem of Counterfeits 11
Definition of Counterfeit 12
III. DoD's Improvement Efforts 17
Current Policies, Strategies, & Procedures 17
IV. Private Sector, Security Best Practices, and Models 26
Emphasizing Symptoms vs. Scenarios 26
Complexity-Criticality Model 26
V. Case Studies and Examples 36
Case #1: Toyota Motors Corp. 36
Case #2: CISCO 40
Results 49
Case #3: McAfee 49
Case #4: NASA 53
VI. Solutions, Implementation Challenges and Lessons Learned 57
Standardizing Risk Assessment and Identification 57
Develop a Process Catalog 63
Nine Security Practices 64
Best Practice Protection against Counterfeits 68
Implementation Challenges 69
Recommendations 72
Benefits of a More Secure Supply Chain at DoD 72
VII. Conclusion 75
Acknowledgements 77
Bibliography 78
About the Authors 86
Appendix 88
Toyota Appendix 90

Table of Figures

Figure 1: Example of Supply Chain Security Risks 4
Figure 2: Least Effectively Managed Supply Chain Components 5
Figure 3: Stock Market Response to Global Events 6
Figure 4: Recent Trends in Supply Chains 7
Figure 5: Visibility Gaps in the Extended Supply Chain 8
Figure 6: Examples of Supply Chain Vulnerabilities 10
Figure 7: Types of DOD Suppliers of Parts and Components 13
Figure 8: Counterfeit Risk 14
Figure 9: OCMs' Top Ten Reasons for Counterfeits Entering the Supply Chain 14
Figure 10: Counterfeit Security Standards in the Works or Under Consideration by DoD 19
Figure 11: Sample Program Protection Plan for IT Acquisition 21
Figure 12: The Product Complexity - Criticality Continuum 27
Figure 13: Embedding Supply Chain Risk Practices Improves Risk Assessment 28
Figure 14: Potential Risks to an Organization and its Supply Chain 30
Figure 15: Heat Map of Risk Events Matrix 31
Figure 16: Locations of Toyota Facilities as of December 2011 36
Figure 17: Structure/Supply Chain of Toyota 37
Figure 18: Earthquake Losses of Sample Electronics and Automotive Companies as of May 2011 38
Figure 19: Cisco's Crisis Management Dashboard 44
Figure 20: Cisco's Revenue Impact 45
Figure 21: Cisco's Resiliency Index Definition 46
Figure 22: GFSC Supplier Assessments Overview 55
Figure 23: Supply Chain Risk Equation 58
Figure 24: Impact and Probability Grid 59
Figure 25: Physical Supply Chain Level of Impact Analysis 60
Figure 26: Supply Chain Security Process Improvement Framework 61
Figure 27: SCSM Operationalized 62
Figure 28: Sample Supply Chain Security Program Elements 63
Figure 29: Holistic Lifecycle-focused Resilience Capability as Risk-reduction Tool 73
Figure 30: Risk Management Innovation Road Map 75
Figure 35: Toyota Plants in Japan 90

Executive Summary

"A supply chain is as secure as its weakest link."

Andreas Wieland, research associate,
Competence Center for International Logistics Networks,
Technische Universität Berlin

The U.S. Department of Defense's (DoD) supply chain is one of the largest, most complex, geographically extended and operationally volatile supply chains in the world. As such, it is at risk from countless existing and potential security threats. These threats range from minimally consequential to potentially catastrophic. They affect the physical flows and products and materials, as well as the information that supports and enables those physical elements. They may compromise missions, endanger lives, or threaten national security. Factors such as globalization, terrorism, and cyber warfare increase DoD's supply chain security risk. There is a pressing need, therefore, for a comprehensive security strategy and practice across DoD's physical and cyber/information supply chains. This is the subject of our report.

Supply chain security is defined as "assured storage and delivery of physical and digital goods and services," but it entails much more than this definition. Supply chain security is also the application of governance and controls that ensure the integrity of the supply chain business process, as well as the material and products in the supply chain. It uses technical and procedural controls to protect the confidentiality, integrity, reliability, and availability of supply chain systems, processes, products carried, and information.[1]

All supply chains face security threats and vulnerabilities. For example, in the physical supply chain, security firm Pinkerton reports that[2]:

- 60 percent of all supply chain security problems involve poor transportation-related security
- 20 percent involve poor security at the manufacturing site, including poor access controls and poor security practices within the shipping and receiving departments
- 90 percent of the time, the security weaknesses were well known internally by staff.

Security Concerns on the Rise

Supply chain security concerns are on the rise in both the public and private sectors. There are a number of reasons for this trend:

- Very few individuals or enterprises focus on the global end-to-end security of the supply chain

[1] "Cyber Threats to National Security, Symposium One: Countering Challenges to the Global Supply Chain." 11. Available at http://asymmetricthreat.net/docs/asymmetric_threat_4_paper.pdf.
[2] Pinkerton Consulting and Investigations, *"Supply Chain Security in 21st Century."* Presentation available at http://www.securitas.com/Global/Pinkerton/Supply%20Chain%20Security.pdf

- The more fragmented and dispersed the supply chain, the greater the security risk
- Very few organizations – including DoD – assess the *entire* chain for security threats and vulnerabilities, analyze the results, or support a common outcome.

For DoD, the evolution of its supply chain during the past two decades – to a highly geographically dispersed network model – has amplified security risk significantly. Reasons include:

- Current supply chain operating practices (e.g., lean, just in time, inventory optimization, outsourcing) reduce costs but create new vulnerability in the DoD supply chain by decreasing flexibility/resiliency
- DoD's reliance on a global supply base puts it at risk from counterfeit parts, supply discontinuity and disruption, quality failures, and so on
- DoD's physical supply chain, because of its global scope/nature and tens of thousands of suppliers/service providers, is at risk for security breaches, terrorist attacks and disruption from disasters/unexpected events
- DoD supply chain's dependence on IT increases vulnerabilities from cyber disruption and attack, malware, security breaches/hacking, compromised components, and compromised networks.

DoD recognizes that it must protect its supply chain while at the same time reduce costs and improving performance. Achieving these frequently conflicting objectives is difficult. Nevertheless, to secure the physical and information/cyber supply chain more effectively, DoD must develop and implement continuous improvement processes that enhance supply chain security, while simultaneously improving performance and reducing costs.

What this Report Covers

In this report, we address the following research questions:

- What is the state of DoD's supply chain security challenge – current and potential vulnerabilities?
- What are the current and potential impacts of these vulnerabilities?
- What steps has DoD taken to address supply chain security?
- What are commercial "best practices" for securing the supply chain?
- What can/should DoD do to further address supply chain security issues and priorities?

The report is divided into seven sections:

Part I provides an overview of the issues and challenges in managing supply chain security at DoD.

Part II delves into security and the physical supply chain, looking at specific risk areas such as sourcing/supply base management, counterfeit parts, production-related vulnerabilities, transportation, and warehousing/inventory management/distribution. It reviews the current and potential impact of these vulnerabilities.

Part III reports on how DoD is addressing its supply chain security issues. It includes a summary of current policies, strategies and procedures aimed at improving supply chain security, and a look at the efficacy and impact of these efforts. It also covers issues relating to security and the cyber/information supply chain. This includes IT-related breaches and vulnerabilities, visibility black holes and cyber attacks and malware insertions. The section assesses the current and potential impact of these vulnerabilities.

Part IV highlights how private industry and other USG agencies address supply chain security risk management. This section presents best practices and models, standards, successes/failures and lessons learned.

Part V offers case studies and examples of supply chain security issues and practices at work in organizations such as Toyota, Cisco, McAfee and NASA.

Part VI looks at what practices/models DoD could adopt to improve supply chain security in a cost effective manner, and what impact the changes could produce. It also looks at implementation challenges for DoD in improving supply chain security. Finally, the chapter discusses lessons learned – from both the private and public sectors – in implementing change.

Part VII concludes the report with overall observations and recommendations about supply chain security at DoD going forward.

Introduction & Focus

DoD buys products and services from a wide variety of firms; these include domestic and international commercial and mixed defense and non-defense companies that service many customers – both within and outside of defense markets.

DoD's efforts to source from defense-unique to commercial companies is typically in the best interest of the warfighter and the taxpayer. Buying from commercial sources and taking advantage of commercial technology in areas like IT incorporates more innovative products into the military's arsenal, and it does so at a lower cost to the taxpayer. It also injects more competition into the buying process and allows for quicker integration of technology improvements into weapons systems.

"Foreign competition pushes our domestic base to continue producing innovative, cutting-edge products that can compete with new international entrants, fomenting competition in price and capabilities throughout the vender base. It allows the Department to benefit from a broader base of R&D and capital investments, augmenting our own investments that draw on the U.S. government budget. Sharing technologies and processes among allies also helps ensure that when we engage around the world, our systems are interoperable to the greatest extent possible."

At the same time, the commercial base has become increasingly global in nature. It maintains global supply chains, gets financing from global investors, and employs a global workforce. This is a fact of business life today.

In addition to the risk already inherent in the increasingly distributed and networked domestic supply chain, this globalization increases the complexity, and therefore the risks in the area of supply chain security. Reliance on multiple parts/players in diverse locations also reduces visibility and adds latency into monitoring systems. The issue of counterfeit parts, for example, has always existed at DoD. But with a globally extended supply chain, it becomes more difficult to prevent introduction of such parts when suppliers are spread across the world.

Complex, highly distributed and interconnected supply chains also can face greater risk of disruptions. Natural disasters, for instance, can happen anywhere in the world, and even an entirely domestic defense supply chain can face major disruptions from such events – as evidenced by the recent devastating impact of Hurricane Sandy on New York and New Jersey. "But if a disruption occurs at a domestic supplier, the Department [of Defense] can use Defense Priorities and Allocation authorities under the Defense Production Act to compel U.S. industry to prioritize DoD critical orders. Those authorities do not extend overseas, so when disruptions occur at foreign suppliers, the Department may have a more difficult time adjusting."

The other exacerbating problem with a highly distributed supply chain is visibility – or lack thereof. Supply chains today operate with multiple tiers of suppliers and service providers all performing activities to support their own enterprises and serve their customers, and all

connected by the thread of their common business. In this environment, supply chains generally are managed in discrete segments – with segments frequently operating independently and in isolation from each other. The result is a lack of overarching visibility that extends across the entire supply chain and all of its 'actors' or participants. In most cases, visibility in the supply chain extends only to the immediate next tier – meaning that an organization may have visibility into its tier 1 or immediate suppliers, but no visibility into its supplier's suppliers.

This lack of visibility, which occurs even in an entirely US-domestic supply chain, has major implications for security. At a 2010 cyber symposium the former U.S. Department of Homeland Security, Hon. Tom Ridge commented on just one aspect of this situation:

"There are very few acquisition systems that track an end item completely through the supply chain. Most program offices, manufacturers, and vendors see their responsibility as taking material from their supplier, performing the operations that they are (contractually or officially) responsible for, and delivering that product to the next stage in the supply chain.

The group that manufactures silicon chips usually does not know, or really care, whether the chips are going into a low-power radar amplifier or a high-speed computer, as long as they pass their factory acceptance test. The manufacturer has little interest if a box of silicon chips sits unguarded in a railroad siding for three weeks. As long as it gets to the next producer in the supply chain by the contractual delivery date, the chip manufacturer and their customer are content.

The same is true for the manufacturer of the low-power amplifier. Along the supply chain, no one may know or care if the amplifier is going on a ship, an airplane, or a land-based station. No great importance is attached to the fate of this amplifier once it passes the factory acceptance test and is delivered to the radar manufacturer in accordance with the terms and conditions of the subcontract.

Absent detailed, objective knowledge of the entire chain, if there is no assessment of the security of all the suppliers, customers, interfaces, and every link in the chain, it is not possible to truly know where security investment dollars are going. Very few organizations assess the entire chain for weaknesses, analyze the results, or support a common outcome."

Given these realities, it seemed appropriate to undertake an assessment of the current state of defense supply chain security. This research paper, therefore, looks at the issues around supply chain security at DoD and what opportunities exist to improve protection of both the material and information that transits the DoD supply chain.

I. Overview: Supply Chain Security and DoD

Definition of Supply Chain Security

To begin our analysis of supply chain security at DoD, let us first define the term. According to David Closs et al. of Michigan State University, supply chain security is:[3]

> *"The application of policies, procedures, and technology to protect supply chain assets (product, facilities, equipment, information, and personnel) from theft, damage, or terrorism, and to prevent, the introduction of unauthorized contraband, people, or weapons of mass destruction into the supply chain."*

According to ISO 28000, security in a supply chain can be defined as "resistance to intentional, unauthorized act(s) designed to cause harm or damage to, or by, the supply chain."[4]

"Supply chain assets," Closs continues, "are defined as not only the equipment and facilities used to carry out supply chain processes, but also the product, information, and human resources required to operate the supply chain."[5] Therefore, supply chain protection does not stop with securing a facility through gates and locks. It extends to the protection of products and people involved in supply chain activities, as well as the internal and external information flows across the supply chain. Second, supply chain defense is not simply a matter of ensuring the safety of these assets, but also preventing theft, damage, and unintended intrusions that could disrupt supply chain operations.[6]

Any definition must incorporate three unique, but interrelated constructs: risk, protection, and safety. A firm or supply chain implements security measures to protect against potential risks. A risk involves the assessment of the likelihood and magnitude of a possible event that could result in a loss for the organization. Risks include those that are internal to the supply chain - supplier facility destruction, supplier bankruptcy, labor disputes, and other factors; or external to the supply chain, such as natural disasters, acts of war, and acts of terrorism.[7]

Supply chain security attempts to render a supply chain less vulnerable to risk and is essential for two reasons. First, organizations need to prevent loss from theft or damage. Second, they need to prevent unauthorized intrusion into shipments that could enable insertion of contraband (drugs, weapons, bombs, human trafficking, counterfeit goods, etc), loss of intellectual property or technology contained in the shipments, and tampering (insertion of harmful elements such as

---

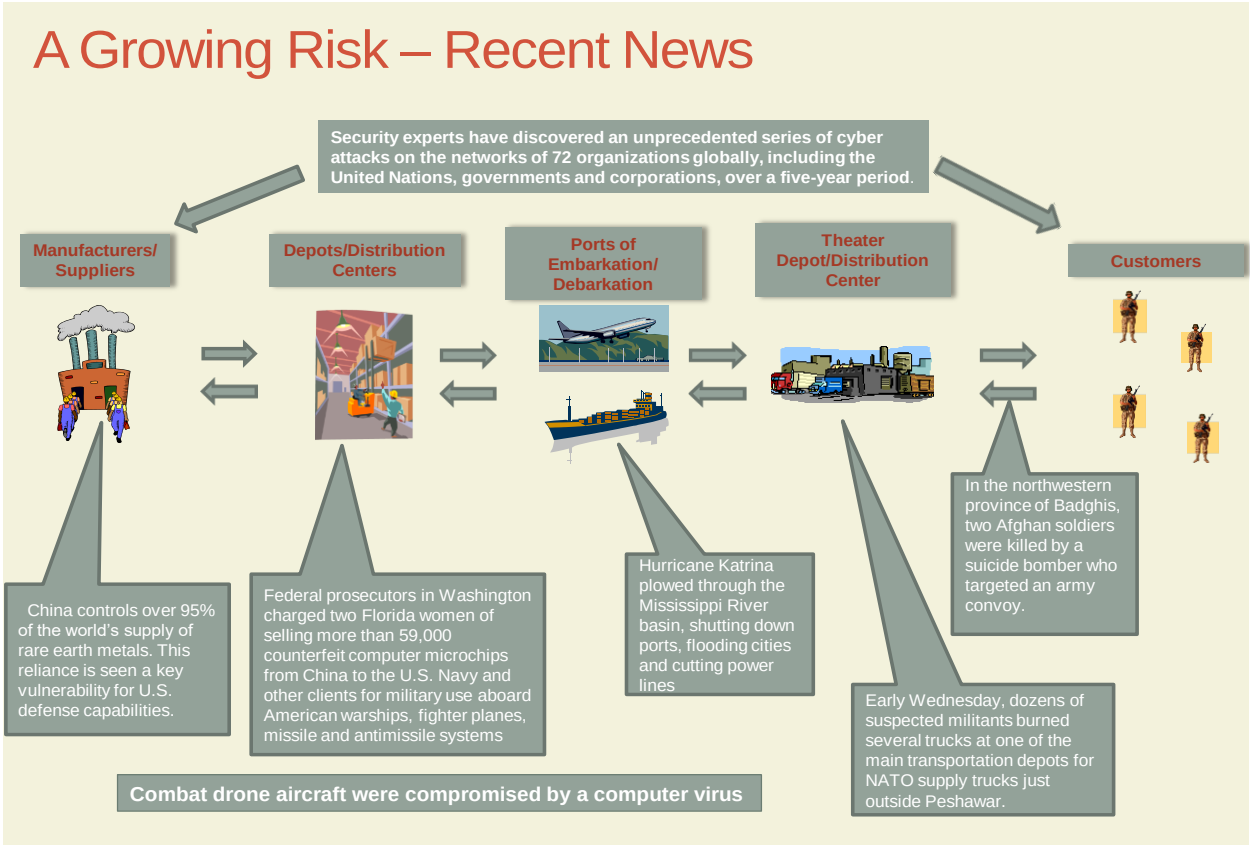
[3] Closs, David, Cheri Speier, Judith Whipple, and M. Douglas Voss. "A Framework for Protecting Your Supply Chain." *Logistics Management (Highlands Ranch, CO)*, March 2008, 38. Accessed September 17, 2012. http://www.highbeam.com/doc/1G1-185243775.html.
[4] Supply Chain Risk Leadership Council. "Supply Chain Risk Management: A Compilation of Best Practices." August 2011, 4. Accessed September 13, 2012. Available at http://www.scrlc.com/articles/Supply_Chain_Risk_Management_A_Compilation_of_Best_Practices_final[1].pdf
[5] Closs, David, Cheri Speier, Judith Whipple, and M. Douglas Voss. "A Framework for Protecting Your Supply Chain." *Logistics Management (Highlands Ranch, CO)*, March 2008, 38. Accessed September 17, 2012. http://www.highbeam.com/doc/1G1-185243775.html.
[6] Ibid.
[7] Ibid.

poisons or "Trojan horses" in computing goods). Supply chain security also must address disruption.[8]

Effective supply chain security and protection includes basic standards for physical security, access controls, personnel security, education and training, procedural security, information-technology (IT) security, business-partner security, and conveyance security from the point of origin to final destination within your supply chain.[9]

Because a supply chain is a system in which any break or breakdown can lead to the collapse of the entire supply chain, it is critical to adopt a holistic approach to the topic.

Figure 1: Example of Supply Chain Security Risks



Source: Center for Public Policy and Private Enterprise 2012.

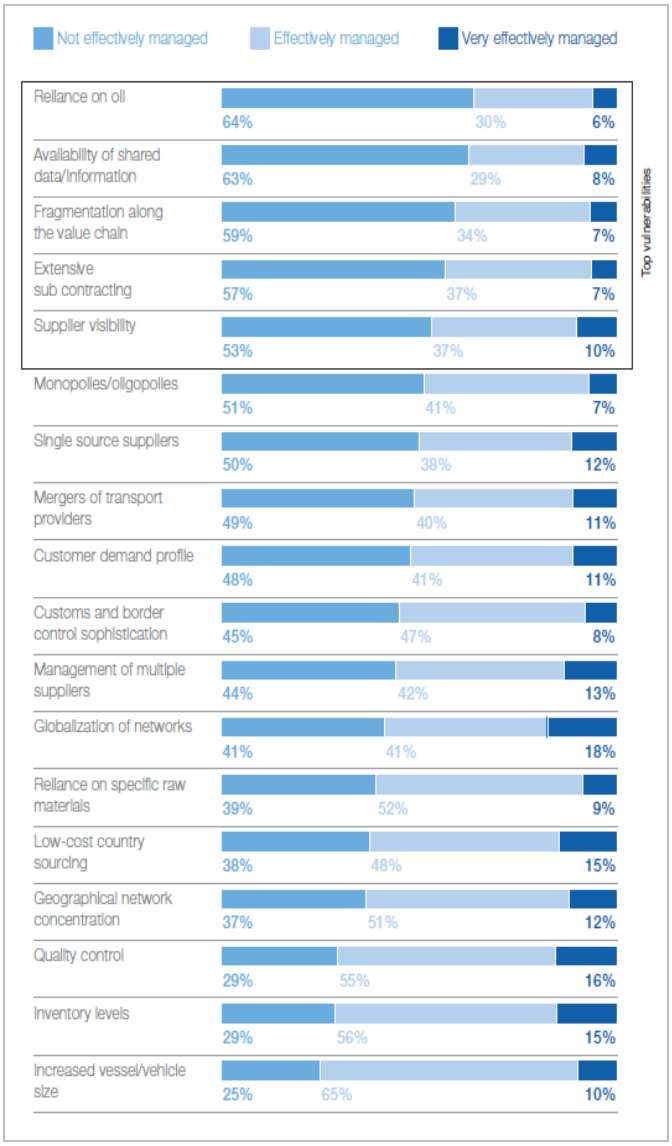
"Security can be achieved in the entire supply chain only if it is borne in mind at an early stage when planning the supply chain design to attach security as a fundamental feature," asserts Wieland. "Furthermore, security must not be forgotten in the company's everyday life, since

[8] Supply Chain Risk Leadership Council. "Supply Chain Risk Management: A Compilation of Best Practices." August 2011, 19. Accessed September 13, 2012. Available at http://www.scrlc.com/articles/Supply_Chain_Risk_Management_A_Compilation_of_Best_Practices_final[1].pdf

[9] Ibid.

even small security gaps may lead to tremendous harm, if they allow a perpetrator to destroy a building, steal freight, or even cause casualties. Supply chain security therefore needs to simultaneously address both the entire supply chain (the holistic view) and its constitutive elements (the atomic view). It must focus on programs, procedures, systems, technology product and especially people."[10] (Figure 1 depicts examples of supply chain security risks and illustrates the breadth of exposure.)

Figure 2: Least Effectively Managed Supply Chain Components



Source: World Economic Forum. "New Models for Addressing Supply Chain and Transport Risk." Geneva, Switzerland, 2012, 11. Accessed August 1, 2012. Presentation available at http://www.weforum.org/reports/new-models-addressing-supply-chain-and-transport-risk.

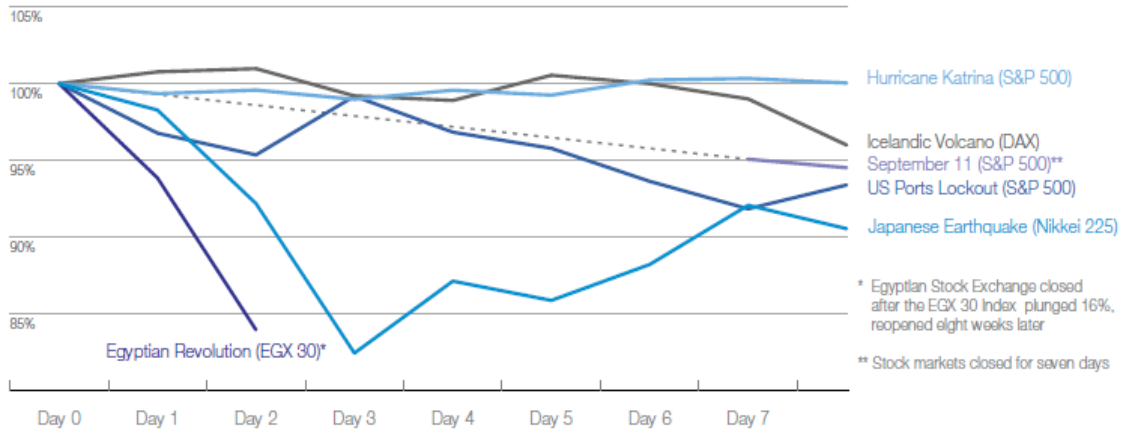
Supply chain and transport network vulnerabilities can magnify the impact of disruption. Recognizing this fact, the World Economic Forum recently identified supply chains and transport networks, in terms of their current management, and capacity to magnify the impact of external disruptions (Figure 2). Four of the top five areas of vulnerability relate to visibility and control along long and complex supply chain networks. Three of the top five vulnerabilities deal with managing the five most concerning aspects of multiple players in the ecosystem.[11]

In a broader context of risk management, supply chain security problems can have a tremendous impact on an organization. For example, during the Egyptian uprising, the EGX 30 Index fell 16 percent in two days, while the Japanese earthquake and tsunami resulted in the Nikkei Index dropping 10.6 percent. Following the reopening of the stock markets seven days after the 11 September terrorist attack, the S&P lost 11.6 percent over the subsequent four days (Figure 3).[12]

[10] Wieland, Andreas. "Strategic Supply Chain Security." *Journal of Homeland and Security* volume # (2009): pages?
[11] World Economic Forum. "New Models for Addressing Supply Chain and Transport Risk." Geneva, Switzerland, 2012, 11. Accessed August 1, 2012. Presentation available at http://www.weforum.org/reports/new-models-addressing-supply-chain-and-transport-risk.

[12] Ibid, 12.

Figure 3: Stock Market Response to Global Events



Source: World Economic Forum. "New Models for Addressing Supply Chain and Transport Risk." Geneva, Switzerland, 2012, 12. Accessed August 1, 2012. Presentation available at http://www.weforum.org/reports/new-models-addressing-supply-chain-and-transport-risk.

Why Security Risk is Increasing

The evolving nature of supply chain networks and business models has altered risk distribution for organizations. The focus on cost optimization through such strategies as offshoring, outsourcing, just in time, and 'lean' has reduced cost significantly. However, removing traditional buffers such as safety stock and excess capacity simultaneously increased risk. Figure 4 shows how specific supply chain practices have impacted organizational risk profiles. In every case, even the best practice adopted increased risk.[13]

Figure 4: Recent Trends in Supply Chains

Trend	Example	Risk Impact
Globalization	Outsourcing, offshoring	Local concentrated risks become globally diffused, involving multiple actors
Specialization	Geographical concentration of product	Efficient process can be easily disrupted by localized event
Complexity	Product/network complexity	Reliance on multiple parts/players in diverse locations reduces visibility and adds latency into monitoring systems
Lean processes	Single sourcing, buffer stock	While initially efficiency is improved and costs are lowered, fewer alternatives in case of disruption
Information availability	Track	Systems heavily reliant on information flow in order to operate
Government legislation	Air cargo screening, C-TPAT	Measures can impede efficient flow of supply chain and transport networks

Source: World Economic Forum. "New Models for Addressing Supply Chain and Transport Risk." Geneva, Switzerland, 2012, 10. Accessed August 1, 2012. Presentation available at http://www.weforum.org/reports/new-models-addressing-supply-chain-and-transport-risk.

The electronics and high tech equipment sector is an excellent example of the impact of globalization and cost optimization. Today, fewer and fewer electronics and high tech original equipment manufacturers (OEMs) manufacture their own products, preferring instead to outsource production to third parties.

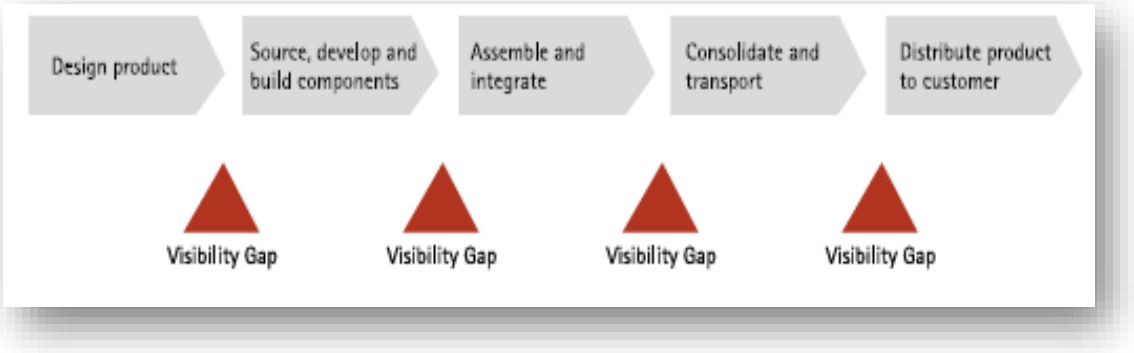
"The rise of contract manufacturers and eventually original design manufacturers (ODMs) made the outsourcing of manufacturing DoD is an appealing proposition for cost and capital focused OEMs," writes Craig Gottlieb of Accenture. "Analysts estimate that by 2013, ODMs will produce nearly 70 percent of portable media players, LCD TVs, digital still cameras, video game devices and digital set-top boxes."[14]

[13] Ibid., P. 10

[14] Gottlieb, Craig, "Securing Goods Across the Supply Chain: Closing the Gaps in the Manufacturing Supply Chain to Achieve High Performance." Accenture, 2010, 3. Accessed September 17, 2012. Available at http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Securing_Goods_Across_the_Supply_Chain.pdf.

This high level of outsourcing has increased supply chain complexity. Gottlieb goes on to say, "As OEMs outsource to ODMs, contract manufacturers (CMs) and electronic manufacturing services (EMS), these subcontractors turn to other suppliers for components, which in turn source the raw materials from yet another set of suppliers. The result is a multi-tier, global supply chain. OEMs are finding that while highly outsourced, multi-tier, global supply chains reduce manufacturing costs, they are complex and difficult to manage. OEMs may have good visibility into their first and second tiers of suppliers, but beyond that, the view becomes murky. This lack of visibility to the lowest, or "nth", tier of suppliers complicates demand planning, inventory planning, sales and operations planning, logistics, transportation management and other areas of supply chain management."[15] Figure 5 depicts these visibility gaps.

Figure 5: Visibility Gaps in the Extended Supply Chain



Source: Gottlieb, Craig, "Securing Goods Across the Supply Chain: Closing the Gaps in the Manufacturing Supply Chain to Achieve High Performance." Accenture, 2010, 3. Accessed September 17, 2012. Available at http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Securing_Goods_Across_the_Supply_Chain.pdf.

At the lowest end of the product risk scale—low complexity, low criticality—most OEMs already have some version of the necessary tools in place. Rigorous sourcing processes with requests for proposal that evaluate long term quality, regularly scheduled audits and long term supplier relationships are typically adequate safeguards for these products.[16] At the higher end of the complexity criticality range, a more significant investment in process and technology is required to provide high levels of supply chain security.[17]

"The n-tier (multi-tier) supply chain, while bringing down manufacturing costs, has opened multiple entry points for product quality to be compromised," Gottlieb notes. "Poor quality and off-spec materials, counterfeit components and corrupted embedded software are symptoms of this widening gap in security."[18]

[15] Ibid, 3.
[16] Ibid., 8.
[17] Ibid.
[18] Ibid., 3.

All too often OEMs in the high tech sector and elsewhere are managing complex, n-tier supply chains with outdated policies designed for managing the simpler, more direct supply chains of just a few years ago. These include:[19]

- Maintaining central control over supplier selection and management
- Relying on original design manufacturers and contract manufacturers to protect against security breaches further down the supply chain
- Conducting internal audits to ensure quality. Few OEMs and primary suppliers have the global presence to adequately monitor the furthest reaches of a complex supply chain that may include thousands of components, twenty or more partners and multiple transportation legs.

As we discuss in the next section, DoD experiences exactly the same kinds of issues and behaviors in managing its supply chain, and the security and integrity of the products it carries.

[19] Ibid.

II. DoD's Supply Chain Vulnerabilities

Because DoD has adopted the same business practice as industry in an effort to drive out cost and improve efficiency, the agency now finds itself vulnerable to the same kinds of security threats along its massive supply chain. A 2012 GAO report, for example, characterized vulnerabilities in DoD acquisition of IT products. Figure 6 describes the types of vulnerabilities that could be exploited in the acquisition of information security products.[20]

Figure 6: Examples of Supply Chain Vulnerabilities

Vulnerability	Description	Threat Example
Acquisition of information technology products or parts from independent distributors, or brokers	Purchasing from a source other than an original component manufacturer or authorized reseller may increase an agency's risk of encountering substandard, subverted, and counterfeit products.	Installation of counterfeit hardware or software.
Incomplete information on IT suppliers	Acquiring IT equipment, software, or services from suppliers without understanding the supplier's past performance or corporate structure may increase risk of (1) encountering substandard, subverted, and counterfeit products, or (2) providing adversaries of the United States with access to sensitive agency systems or information. For example, lacking information concerning an IT service provider's corporate structure could reduce an agency's ability to assess whether or not the service provider or its employees are subject to undue foreign control or influence	• Installation of hardware or software containing malicious logic or unintentional vulnerabilities • Installation of counterfeit hardware or software
Use of supply chain delivery and storage mechanisms that are not secure	Using delivery or storage mechanisms that are not secure may increase the risk that an IT product is intercepted or subverted while it is in transit to the agency or while it is in storage before installation. This vulnerability may allow a threat actor to gain unauthorized access to the IT product, thereby facilitating unauthorized modification, substitution, or diversion. Unsecured delivery and storage mechanisms may also lead to the exposure of sensitive information to unauthorized parties, such as the identity of the agency purchasing the IT product or how the IT product will be used.	• Failure or disruption in the production • Product tampering • Product diversion or theft • Delivery failures

Source: United States Government Accountability Office. *"National Security – Related Agencies Need to do Better."* GAO-12-361, March 2012

[20] United States Government Accountability Office. *"National Security – Related Agencies Need to do Better."* GAO-12-361, March 2012, 16-17.

The Issue of Rare Earth Metals

Rare earth materials—rare earth ores, oxides, metals, alloys, semi-finished rare earth products, and components containing rare earth materials—are used in a variety of commercial and military applications, such as cell phones, computer hard drives, and Department of Defense (DOD) precision-guided munitions. Some of these applications rely on permanent rare earth magnets that have unique properties, such as the ability to withstand demagnetization at very high temperatures.

The National Defense Authorization Act for Fiscal Year 2010, Section 843, directed GAO to submit a report on rare earth materials in the DOD supply chain.

While rare earth ore deposits are geographically diverse, current capabilities to process rare earth metals into finished materials are limited mostly to Chinese sources.

The United States previously performed all stages of the rare earth material supply chain, but now most rare earth materials processing is performed in China, giving it a dominant position that could affect worldwide supply and prices.

Based on industry estimates, rebuilding a U.S. rare earth supply chain may take up to 15 years and is dependent on several factors, including securing capital investments in processing infrastructure, developing new technologies, and acquiring patents, which are currently held by international companies.

DoD's concern lies with the fact that China and other countries to a less degree, control the world supply of materials that are critical in many weapons systems and products.

Martin, Belva M. United States Government Accountability Office. "Rare Earth Materials in the Defense Supply Chain." April 1, 2010, 4-5, 14-16.

The Problem of Counterfeits

One security issue that is particularly concerning to DoD is counterfeits. Counterfeit parts have always been a concern for the agency. DoD's globally extended acquisition chain, however, has resulted in a significant increase in the volume of counterfeits in the DoD supply chain. A 2010 report by the U.S. Department of Commerce discussed this issue:[21]

"In June 2007, the U.S. Department of the Navy, Naval Air Systems Command (NAVAIR) asked the Bureau of Industry and Security's (BIS) Office of Technology Evaluation (OTE) to conduct a defense industrial base assessment of counterfeit electronics. NAVAIR suspected that an increasing number of counterfeit/defective electronics were infiltrating the DoD supply chain and affecting weapon system reliability.

OTE surveyed five segments of the U.S. supply chain – original component manufacturers (OCMs), distributors and brokers, circuit board assemblers, prime contractors and subcontractors, and Department of Defense (DOD) agencies. The objectives of the survey were to assess: levels of suspected/confirmed counterfeit parts; types of devices being counterfeited; practices employed in the procurement and

[21] U.S. Department of Commerce: Bureau of Industry and Security: Office of Technology Evaluation. "Defense Industrial Base Assessment: Counterfeit Electronics." January 2010, i-ii. Available at http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf.

management of electronic parts; recordkeeping and reporting practices; techniques used to detect parts; and best practices employed to control the infiltration of counterfeits.

OTE data revealed that 39 percent of companies and organizations participating in the survey encountered counterfeit electronics during the four-year period. Moreover, information collected highlighted an increasing number of counterfeit incidents being detected, rising from 3,868 incidents in 2005 to 9,356 incidents in 2008.

The rise of counterfeit parts in the supply chain is exacerbated by demonstrated weaknesses in inventory management, procurement procedures, recordkeeping, reporting practices, inspection and testing protocols, and communication within and across all industry and government organizations."

Definition of Counterfeit

OTE developed a broad definition of the term "counterfeit" to encompass the views of different segments of the supply chain. For this assessment, a counterfeit is an electronic part that is not genuine because it:[22]

- is an unauthorized copy
- does not conform to original OCM design, model, and/or performance standards
- is not produced by the OCM or is produced by unauthorized contractors
- is an off-specification, defective, or used OCM product sold as "new" or working or
- has incorrect or false markings and/or documentation

All elements of the supply chain have been directly impacted by counterfeit electronics, and the threat of counterfeit parts continues to grow as counterfeiters have developed more sophisticated capabilities to replicate parts and gain access to scrap materials that were thought to have been destroyed.[23]

Counterfeiting can affect the safety, operational readiness, costs, and the critical nature of the military mission. DOD procures millions of parts through its logistics support providers—DLA supply centers, military service depots, and defense contractors—who are responsible for ensuring the reliability of the DOD parts they procure. As they draw from a large network of suppliers in an increasingly global supply chain, there can be limited visibility into these sources and greater risk of procuring counterfeit parts.[24]

Also, as DOD weapon systems age, products required to support it may no longer be available from the original manufacturers or through franchised or authorized suppliers. Additionally, says the Commerce Department report, "DOD logistics offices in charge of solving obsolescence

[22] Ibid., 3-4.
[23] Martin, Belva. United States Government Accountability Office. "Defense Supplier Base DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts." GAO-10-389, March 2010, 2. Available at http://www.gao.gov/assets/310/302313.pdf.
[24] Ibid.

problems are challenged by limited budgets, procurement issues, and time issues. It is typically less expensive to find part substitutions and aftermarket manufacturing for needed electronic parts than reengineering and redesigning parts and components. Obsolescence mitigation strategies also take a long time to implement. These factors can force procurement agents to purchase parts from unknown sources, which can introduce counterfeit parts into weapon systems."[25]

Obsolete components are not the only parts being counterfeited, the OTE survey found. There are also counterfeit versions of the newest parts and components currently being manufactured by OCMs. This increases the difficulty that procurement agents in industry and the government face when trying to locate authentic, dependable parts.[26] Instead, DoD must acquire them from independent distributors, brokers, or aftermarket manufacturers. Parts and components bought by DOD can come from different types of suppliers, as shown in Figure 7.[27]

Figure 7: Types of DOD Suppliers of Parts and Components

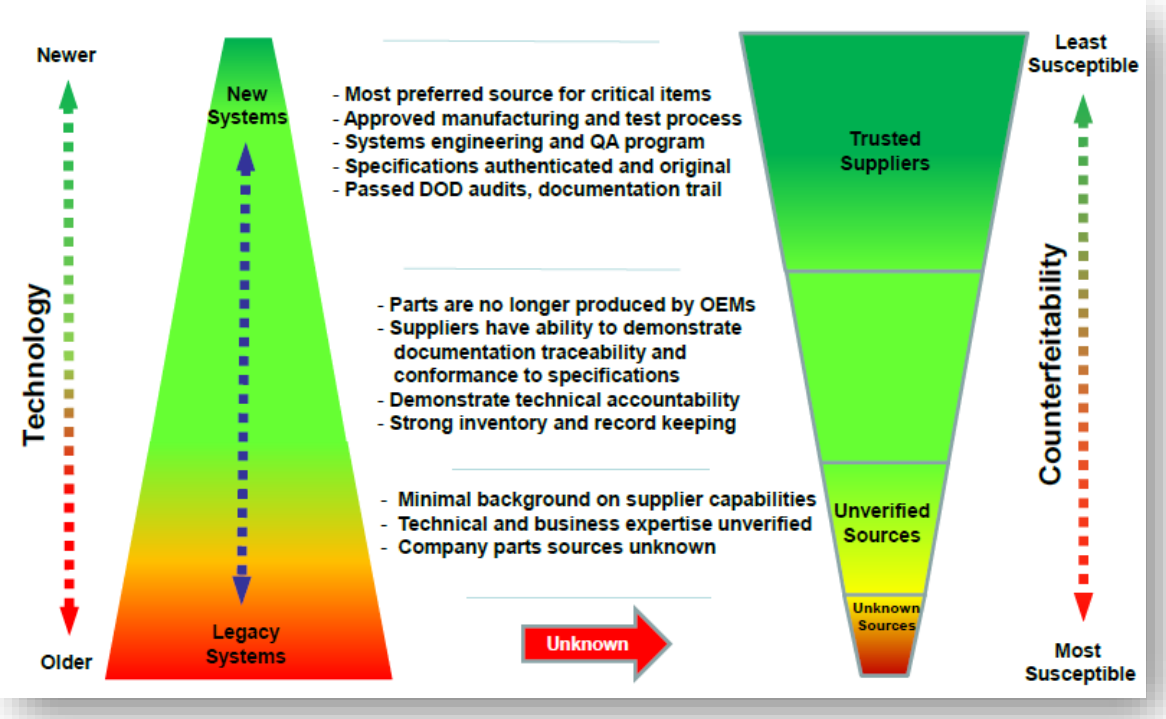
Type of Source	Description
Original component manufacturer (OCM)	Organization that designs, or engineers, or both, a part and is pursuing or has obtained the intellectual property rights to that part.
Franchised distributor	Distributor with which OCM has a contractual agreement to buy, stock, repackage, sell and distribute its product lines.
Independent Distributor	Distributor that purchases new parts with the intention to sell and redistribute them back into the market, and which does not have contractual agreements with OCM.
Broker/ broker distributor	In the independent distribution market, brokers are professionally referred to as independent distributors. A broker distributor is a type of independent distributor that works in a just-in-time environment by searching the industry and locating parts for customers.
Aftermarket Manufacturer	Manufacturer that either (1) produces and sells replacement parts authorized by the OCM, or (2) produces parts through emulation, reverse-engineering, or redesign that match OCM specifications and satisfy customer needs without violating OCM intellectual property rights, patents, or copyrights.

Source: Martin, Belva. United States Government Accountability Office. "Defense Supplier Base DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts." GAO-10-389, March 2010, 3. Available at http://www.gao.gov/assets/310/302313.pdf.

Figure 8 illustrates the dramatic effect aging systems and platforms have on the DoD's risk of acquiring counterfeit replacement parts.

[25] U.S. Department of Commerce: Bureau of Industry and Security: Office of Technology Evaluation. "Defense Industrial Base Assessment: Counterfeit Electronics." January 2010, 1-2. Available at http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf.
[26] Ibid.
[27] Martin, Belva. United States Government Accountability Office. "Defense Supplier Base DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts." GAO-10-389, March 2010, 3. Available at http://www.gao.gov/assets/310/302313.pdf.

Figure 8: Counterfeit Risk



Source: Peters, Paul D. "Anti-Counterfeit." Presented to Product Support Manager's Conference by Deputy Assistant Secretary of Defense Supply Chain Integration. June 6, 2012.

The study revealed several key reasons why counterfeits enter the DoD supply chain. Figure 9 lists the top 10 reasons.

Figure 9: OCMs' Top Ten Reasons for Counterfeits Entering the Supply Chain

Greater reliance by brokers on gray market parts	42%
Greater reliance by independent distributors on gray market parts	37%
Less stringent inventory management by parts brokers	36%
Less stringent inventory management by independent distributors	28%
Insufficient buying procedures	23%
Insufficient chain of accountability	27%
Purchase of excess inventory on the open market	23%
Inadequate part purchase planning by OEMs	23%
Inadequate part purchase planning by contract manufacturers	23%
Greater reliance on contract manufacturers for procurement	23%

Source: U.S. Department of Commerce: Bureau of Industry and Security: Office of Technology Evaluation. "Defense Industrial Base Assessment: Counterfeit Electronics." January 2010, 36. Available at http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf.

Reporting Mechanisms for Counterfeit Parts

Government agencies as well as private companies are encouraged to report counterfeits using several databases. The first is the Government Industry Data Exchange Program (GIDEP). GIDEP serves as a data repository for the collection and sharing information on nonconforming parts and materials, including information on suspect counterfeit products government organizations as well as industry partners.[28] This web-based database allows government and industry participants to share information on deficient parts, including counterfeit.

Specifically, a GIDEP user can submit information on a suspected counterfeit part and GIDEP policy allows for up to 15 days for the supplier to respond before posting this information to the database. To ensure that reports are objective and fact based, GIDEP policy requires submitters to notify suppliers of their intention to report. All parties involved are allowed to present their side of the story.[29]

While GIDEP is the predominant counterfeit reporting mechanism in place for government and its suppliers, it is not universally utilized. Studies indicate several reasons why suppliers in particular do not use the system:[30]

- "legal or liability issues (e.g. exposure to third party lawsuits) encumber reporting"
- "my organization's business process does not support reporting non-conforming material findings outside of the organization."

GIDEP issued an interim policy change regarding "Reporting Suspect Counterfeit Parts and Materials" in September 2010 to "facilitate and encourage the reporting of suspect counterfeits until such time as federal policy and an appropriate supporting procedure can be determined and implemented." Under the current GIDEP policy, members are asked to identify the supplier of the part or material when reporting a suspect counterfeit in the database.[31]

However, GIDEP members are "hesitant or not permitted to identify the supplier due to potential legal issues or other concerns." If the "true" manufacturer or supplier is not identified when submitting a report, "current GIDEP policy limits the use … to only a Problem Advisory" and prevents the "reporter from alerting the community via a Safe-Alert or Alert when the severity or likelihood of the failure is known."[32]

---

[28] Livingston, Henry, Teresa Telesco, Lisa Gardner, Ric Loeslein, Ed Zelinski, and William Pumford. "Counterfeit Parts Safeguards and Reporting: U.S. Government and Industry Collaboration to Combat the Threat." *Defense Standardization Program Journal*. January/March 2010: 10, 13.

[29] Martin, Belva. United States Government Accountability Office. "Defense Supplier Base DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts." GAO-10-389, March 2010, 5. Available at http://www.gao.gov/assets/310/302313.pdf.

[30] Aerospace Industries Association of America, Inc. "Counterfeit Parts: Increasing Awareness and Developing Countermeasures." Arlington, Virginia, March 2011, 13-14. Accessed August 1, 2012. http://www.aia-aerospace.org/assets/counterfeit-web11.pdf.

[31] Ibid.

[32] Ibid.

DOD also uses Joint Deficiency Reporting System (JDRS)[33] and the Product Data Reporting and Evaluation Program (PDREP)[34] for reporting and disposal of deficient parts. JDRS and PDREP do not have a specific field in which to report counterfeit parts, however, some DOD officials stated that they report suspect counterfeits to internal fraud teams, others indicated that they would contact local law enforcement or the Federal Bureau of Investigation in similar cases. DOD officials told us that when they found counterfeit parts they have shared this information through informal methods such as e-mails or phone calls. Others use formal methods to convey this information such as bulletins that alert.[35]

[33] JDRS: Joint Deficiency Reporting System is cross-service web enabled automated tracking system designed to initiate, process and track deficiency reports from the Warfighter through the investigation process.

[34] PDREP: The Product Data Reporting and Evaluation Program (PDREP) Automated Information System (AIS) is the Department of the Navy program that supports requirements regarding the reporting, collection and use of supplier performance information identified in the FAR, DFAR and Navy regulations. PDREP provides for Navy management of the supply chain, ensuring the on-time delivery and first time quality of materials for both critical and non-critical applications. PDREP promotes continuous process improvement for increased material readiness and decreased deficiency issues, providing an overall cost savings to DoD and the Navy.

[35] Martin, Belva. United States Government Accountability Office. "Defense Supplier Base DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts." GAO-10-389, March 2010, 9-13. Available at http://www.gao.gov/assets/310/302313.pdf.

III. DoD's Improvement Efforts

Current Policies, Strategies, & Procedures

Supply chain security at DoD is inextricably linked to supply chain risk. Recognizing this fact, in 2003, DoD undertook a program to develop policies and measures to employ in protecting the supply chain. In February 2009, the department issued a policy that requires that supply chain risk be addressed early and across the entire system life cycle. "This policy applies to those systems that handle information that the agency determines is critical—in terms of both content and timeliness—to the readiness or effectiveness of the armed forces. The policy calls for the incremental implementation of supply chain risk management through a series of pilot projects. According to the policy, the target date for achieving full operational capability for supply chain risk management is fiscal year 2016."[36]

In addition, the 2009 policy states that the supply chain pilots shall include, among other things:[37]

- Processes to assess threats from potential suppliers providing critical components to applicable systems
- Processes to detect the occurrence, reduce the likelihood of occurrence, and mitigate the consequences of products containing counterfeit components or malicious functions, and
- Enhanced developmental and operational test and evaluation capabilities, including software vulnerability detection methods and automated tools.

In February 2010, the department released a supply chain risk management Key Practices and Implementation Guide, which describes 32 specific measures that an organization could take to enhance supply chain protection. According to these procedures, program protection plans should guide a program office's security measures, and should be updated as threats and vulnerabilities change or are better understood.[38]

The procedures identify at least four ways in which Defense programs should manage supply chain risk. The focus is on developing and assuring a trusted network of suppliers. The procedures are geared toward protecting the supply chain software and IT areas primarily but could easily be applied in a broader supply chain context. The procedures recommend that program officials:[39]

- Identify critical program information, critical functions, and components[40]

---

[36] United States Government Accountability Office. "*National Security – Related Agencies Need to do Better."* GAO-12-361, March 2012, 21. Available at http://www.gao.gov/assets/590/589568.pdf.
[37] Ibid, 22.
[38] Ibid.
[39] Ibid., 23.
[40] NOTE: Defense defines "critical program information" as elements or components of a research, development, and acquisition program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability.

- Document how supply chain threat assessments will be used to influence system design, development environment, and procurement practices
- Assess the need for trusted suppliers for integrated circuits, and
- Identify specific counterfeit protection measures.

A July 2011 memorandum, which was issued by the Principal Deputy Under Secretary of Defense for Acquisition, Technology, and Logistics, requires every acquisition program to submit and update a "program protection plan" (PPP) at each milestone of Defense's system acquisition process. Program protection is intended to be the integrating process for managing risks to advanced technology and mission-critical system functionality from supply chain vulnerabilities throughout the acquisition life cycle.[41]

> *"At its core, program protection protects technology, components, and information from compromise through the cost-effective application of countermeasures to mitigate risks posed by threats and vulnerabilities. In a simple sense, program protection seeks to defend warfighting capability by 'keeping secret things from getting out' and 'keeping malicious things from getting in.' Where the capability is derived from advanced or leading-edge technology, program protection mitigates the risk that the technology will be lost to an adversary; where the capability is derived from integration of commercially available or developed components, program protection mitigates the risk that design vulnerabilities or supply chains will be exploited to degrade system performance."*[42]

The process of preparing a PPP is intended to help program offices consciously think through what needs to be protected and to develop a plan to provide that protection, states the DoD. "Once a PPP is in place, it should guide program office security measures and be updated as threats and vulnerabilities change or are better understood," DoD's PPP guidance says. "External, interdependent, or government furnished components that may be outside a program managers' control must be considered.[43]

Furthermore, according to DoD's Trusted Mission Systems and Networks officials, the department is collecting metrics to assess the effectiveness of the supply chain risk management aspects of protection planning. "Specifically," says the GAO report on national security, "officials stated that the department is collecting data concerning the extent to which the department has engaged with program managers to understand supply chain threats, conducted criticality analyses to identify critical functions, and developed appropriate countermeasures and

[41] Ibid, 22.
[42] United States Department of Defense. "Chapter 13: Program Protection Plan." Defense Acquisition Guidebook, p 1. Accessed October 15, 2012 http://www.ndia.org/meetings/287D/Documents/DAG%20Chapter%2013%20PPP%2003052012.pdf.
[43] Deputy Assistant Secretary of Defense. "Program Protection Plan & Outline Guidance." U.S. Department of Defense. July 2011, 2. Accessed October 17, 2012. Available at http://www.acq.osd.mil/se/docs/PPP-Outline-and-Guidance-v1-July2011.pdf.

mitigations." According to an official within Trusted Mission Systems and Networks, the department had conducted 63 such engagements during fiscal year 2011."[44]

Figure 10 summarizes what standards are either in the works or under consideration at DoD with regard to counterfeit detection, prevention and mitigation as of mid-2012. The chief focus of these standards is on electronic parts and components. We discuss DoD's Trusted Systems and Network Strategy later in this paper.

Figure 10: Counterfeit Security Standards in the Works or Under Consideration by DoD

	Published	Under-Development	Used For Electronic Parts	Used For Procurement Processes & Control	Used For Test and Inspections	Used for Quality Management/ Assurance	Anti-Counterfeit Specifics
AS 5553	X		X	X	X		X
AS 6081		X	X	X		X	X
ARP 6178	X		X	X	X		X
AS 6174		X	X	X	X	X	X
AS 6171		X	X		X		X
ARD 6884		X	X				X
AS 9120/A	X		X			X	
AS 9100	X		X			X	
ISO 9001	X			X		X	
JESD 31	X		X	X		X	

AS 5553 - Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition
AS 6081 - Counterfeit Electronics Parts; Avoidance Protocol, Distributors
ARP 6178 - Fraudulent/Counterfeit Parts; Tool for Risk Assessment of Distributors
AS 6174 - Counterfeit Materiel; Detection, Mitigation, and Disposition
AS 6171 - Test Methods Standards; Counterfeit Electronic Parts
ARD 6884 - Terms and Definition – Fraudulent/Counterfeit Electronic Parts
AS 9120/A - Quality Management System: Requirements for Aviations, Space and Defense Distributors
AS 9100 - Quality Systems – Aerospace – Model for QA in Design, Development, Production, Installation and Servicing
ISO 9011 - Quality Management Standard
JESD 31 - General Requirements For Distributor of Commercial and Military Semiconductor Devices

15

Source: Peters, Paul D. "Anti-Counterfeit." Presented to Product Support Manager's Conference by Deputy Assistant Secretary of Defense Supply Chain Integration. June 6, 2012.

Section 818 – Directive on Counterfeits

On a legislative front, Section 818 of the National Defense Authorization Act of 2012, enacted last December, contains new requirements for the Department of Defense (DoD) to detect and avoid counterfeit electronic parts. While the DoD works to meet Section 818's mandates of assessing current departmental policies and developing specific actions to be taken, the DoD has

[44] United States Government Accountability Office. "*National Security – Related Agencies Need to do Better.*" GAO-12-361, March 2012, 24. Available at http://www.gao.gov/assets/590/589568.pdf.

recently provided guidance to agencies on how to address the growing problem of counterfeit electronic parts in the supply chain.[45]

As part of the assessment process required by Section 818, the Under Secretary of Defense for Acquisition, Technology and Logistics issued a memorandum in March 2012 to the secretaries of the military departments and directors of the defense agencies regarding the DoD's policies related to counterfeit electronic parts. The memorandum directed specific actions to prevent, detect, remediate, and investigate counterfeiting in the DoD supply chain. These actions reinforce Section 818 and stipulate the following:[46]

- Program managers (PMs) must ensure they are notified by the contractors and suppliers – including those below the prime contractor level – when critical items are not obtained from the original equipment manufacturer, original component manufacturer, or an authorized distributor.
- PMs must evaluate counterfeit risk and implement countermeasures for mission critical components, which are outlined in a July 2011 DoD Memorandum entitled "Document Streamlining-Program Protection Plan (PPP)." The PPP should address counterfeit prevention, including what measures will be in place and how the program will mitigate the risk of the insertion of counterfeit parts during operations and maintenance.
- Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.246-7003, "Notification of Potential Safety Issues," must be included in solicitations and contracts for: (1) repairable/consumable parts for critical safety items; (2) systems and subsystems, assemblies, and subassemblies integral to a system; or (3) repair, maintenance, logistics support, or overhaul services for systems and subsystems, assemblies, subassemblies, and parts integral to a system. This DFARS clause sets forth the actions to be taken concerning nonconformance and deficiencies that could result in a critical safety impact.
- GIDEP is designated as the central reporting repository for the DoD for suspected and confirmed counterfeit parts. Contractors, subcontractors, and DoD activities are to report counterfeit parts using the GIDEP's Product Quality Deficiency Reporting process. The counterfeit reports are provided to all GIDEP members and are maintained in an on-line searchable database.

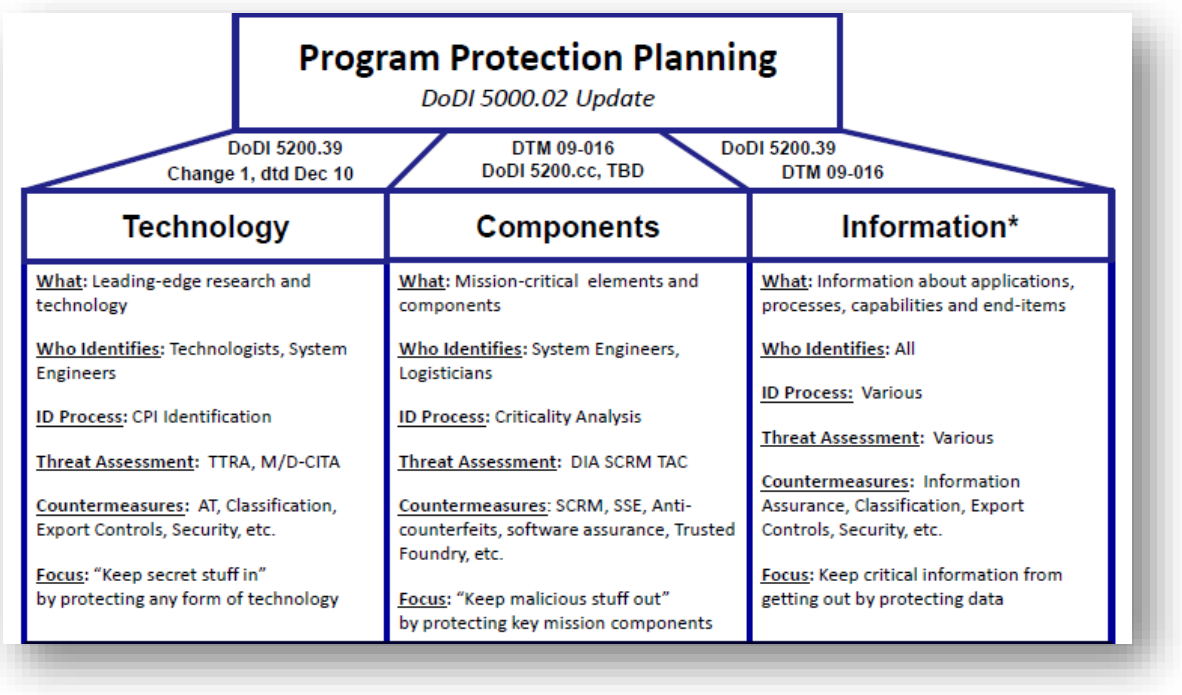
For suppliers, the consequences for failing to report suspected counterfeit electronic parts can be severe, as demonstrated earlier in 2012 when the Air Force suspended two companies and their affiliates from government contracting because of counterfeit electronic parts.

[45] Debolt, Paul A. and George W. Wyatt. "Real Parts: DOD Continues To Develop Policy On Counterfeit Electronic Parts." June 14, 2012. Available at http://www.venable.com/real-parts-dod-continues-to-develop-policy-on-counterfeit-electronic-parts-06-07-2012/.
[46] Ibid.

Section 818 also requires DoD to implement a risk-based policy to minimize the impact of counterfeit electronic parts. The PPP serves this function, and supports the policy requirement for ensuring the traceability of parts, inspecting and testing of parts, and taking corrective action to recover costs for replacing counterfeit electronic parts from contractors.[47] Section 818 also requires DoD to revise the DFARS to address the detection and avoidance of counterfeit electronic parts.

Figure 11 provides a sample PPP for an IT acquisition. The example focuses on asking questions so as to identify vulnerabilities, and highlights appropriate countermeasure options.

Figure 11: Sample Program Protection Plan for IT Acquisition



Source: Fong, E. Kenneth Hong. "Comprehensive Program Protection Planning." Presented at 14th Annual NDIA Systems Engineering Conference. San Diego, CA. October 25, 2011.

Moving forward, DoD plans to continue formalizing its risk-based approach to preventing counterfeits from entering the DoD supply chain. Under this approach, the agency will:[48]

- Improve processes and developing policy for counterfeit prevention and detection.
- Strengthen and standardize existing identification and disposition processes, standards, and contract requirements for counterfeit materiel across industry/DoD supply chain.

[47] Ibid.
[48] Peters, Paul D. "Anti-Counterfeit." Presented to Product Support Manager's Conference by Deputy Assistant Secretary of Defense Supply Chain Integration. June 6, 2012.

- Leverage GIDEP as centralized reporting tool for counterfeit incidents and information sharing.
- Review how to streamline information sharing with allied/coalition countries.

DoD also is standardizing processes across the supply chain so as to keep counterfeits off the production floor. For example, in inventory management, DoD is standardizing processes relating to its materiel control and traceability program, its quality management systems, and its systemic test and verification processes. For disposition of counterfeits in the supply chain, for instance, DoD's processes include holding the counterfeit goods for law enforcement disposition, disposing of materiel according to federal logistics information system code guidance, and executing suspension and debarment process as required.[49] The sidebar below illustrates the kinds of questions managers should investigate in developing a PPP.

Assessing Vulnerability of Critical Components

The questions below are examples of the kinds of factors that should be considered in evaluating the potential vulnerability of a critical component prior to acquisition.

Where and under what conditions was the system designed?
- Who made significant system-wide design decisions?
- Who has had access to design information?
- How are requirements and specifications for critical components communicated to suppliers?
- How much do suppliers know about how critical their products are to the overall system?

Where and under what conditions were critical components developed?
- For custom components, who made significant design decisions?
- Who has had access to design information?
- Where are critical components fabricated or manufactured?
- Who has had access to fabrication or manufacturing processes?
- What testing of critical components has been conducted? How and where?
- How are critical components shipped?
- How has custody of critical components been managed?

How and where are components assembled and integrated into completed systems?
- What final system testing is conducted?

In addition to the above questions, it is useful to assign a criticality level to the overall project. These levels may include:

Level I: Total mission failure
Level II: Significant/unacceptable degradation
Level III: Partial/acceptable degradation
Level IV: Negligible

Source: Fong, E. Kenneth Hong. "Comprehensive Program Protection Planning." Presented at 14th Annual NDIA Systems Engineering

[49] Ibid.

Agencies within DoD have taken specific actions to block the flow of counterfeit products as well. For example, the Defense Logistics Agency's Defense Supply Center Columbus implemented a Qualified Suppliers List Distributors (QSLD) program.[50]

The purpose of the QSLD Program is to establish and maintain a list of pre-qualified sources for certain electronic components that are purchased and managed by DLA Land and Maritime. QSLD products are provided by suppliers that combine accepted commercial practices, quality assurance procedures that are consistent with industry and international quality standards, and tailored when necessary to product-unique requirements that can take the place of provisions traditionally stated in DLA Land and Maritime solicitations.[51]

This approach is designed to reduce the need for testing, engineering reviews, and other activities that can delay acquisitions and increase acquisition costs. The QSLD program also enables DSCC to use automated electronic parts purchasing, but with a modification from past practice. All purchases made through the QSLD system will be subject to a final manual review prior to execution. About 50 percent of parts would be acquired through the system, enabling DSCC to reassign some personnel to other duties.[52]

Trusted Systems and Networks Strategy

In response to the technology supply chain risks, DoD is in the process of institutionalizing the Trusted Defense Systems / Supply Chain Risk Management (SCRM) strategies described in the Report on Trusted Defense Systems in response to the FY09 National Defense Authorization Act (NDAA), Section 254, delivered to the Congress in January 2010. The Department's strategy for achieving trustworthy defense information and weapons systems in light of supply chain risk contains the following core elements: **[53]**

1. **Prioritize scarce resources based on mission dependence** – Allocate the Department's systems assurance resources based on a system's criticality and risk of attack. The difficulty of mounting and defending against supply chain attacks focuses supply chain risk management on sensitive, mission critical systems. Accordingly, DoD policy levies the requirement of trusted systems / supply chain risk processes and practices only on National Security Systems (NSS).

---

[50] U.S. Department of Commerce: Bureau of Industry and Security: Office of Technology Evaluation. "Defense Industrial Base Assessment: Counterfeit Electronics." January 2010, 236-237. Available at http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf.

[51] "QSLD Program (Qualified Suppliers List of Distributors)." Defense Logistics Agency, Land and Maritime, Sourcing and Qualifications. Accessed August 27, 2012. Available at **http://www.landandmaritime.dla.mil/offices/sourcing_and_qualification/offices.aspx?section=QSL.**

[52] U.S. Department of Commerce: Bureau of Industry and Security: Office of Technology Evaluation. "Defense Industrial Base Assessment: Counterfeit Electronics." January 2010, 237. Available at http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf.

[53] Hearing on IT Supply Chain Security: Review of Government and Industry Efforts. March 27, 2012. Before United States House of Representatives Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, 112th Congress, 2nd Session. (statement of Mitchell komaroff, Office of the Department of Defense Chief Information Officer), page 5-6. Accessed November 5, 2012. Available at http://www.hsdl.org/?view&did=704788.

2. **Plan for comprehensive program protection** – Employ comprehensive program protection planning, including systems engineering, supply chain risk management key practices, hardware and software assurance, counterintelligence, test and evaluation and information assurance to identify and protect critical components, functions, technologies, and information using a full range of tools, resources, and practices. DoD's strategy is focused on making these tools, resources, and practices available to protect the most critical functions and components of NSS. DoD requires acquisition programs to perform criticality analysis, by which they identify mission-critical functions and components, down to the commercial hardware, software, and firmware components that implement those functions.
3. **Partner with industry** – Collaborate with industry to develop commercially reasonable standards for global sourcing and SCRM and to identify leading edge commercial practices and tools.
4. **Incremental Implementation -** DoD is adopting a SCRM approach to manage acquisitions. Supply Chain Risk Management (SCRM) represents a change in the acquisition process. It requires new institutional relationships between acquisition and the intelligence community.

DoD has conducted a number of pilot tests in applying SCRM strategy in its acquisitions processes. DoD is currently institutionalizing lessons learned during the piloting phase into permanent policy and practice.[54]

- First, the DIA mission to support DoD acquisition with supply chain threat analysis has been made permanent in DoD Instruction (DoDI) 5240.24, June 8, 2011, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)." To date, DIA TAC has performed approximately 520 analyses for DoD acquisition programs.
- Other key tenets were institutionalized on July 18, 2011, when the Principal Deputy USD(AT&L) issued a Memorandum to all DoD Component Acquisition Executives directing that Program Protection Plans (PPP) incorporate key elements of the above Trusted Defense System/SCRM Strategy, including criticality analysis, use of DIA TAC analyses, SCRM Key Practices, and hardware and software assurance. To help institutionalize the prioritization process, DoD developed a rigorous Criticality Analysis methodology and has engaged over 60 programs to implement it. In addition, over 25 major system acquisitions have incorporated SCRM into their PPPs.
- We will further institutionalize the concepts we piloted through the DoDI 5200.MM, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks." That instruction, in the final stages of coordination, will be signed out by the DoD CIO and the USD(AT&L), and will make the Trusted Defense Systems/SCRM Strategy outlined above and issued in the DTM 08-048 permanent. It requires that risks to critical

[54] Ibid., 6-9

> functions and components of mission-critical systems be protected across the entire system lifecycle, and is the policy that will enable full operating capability for SCRM across the Department. DoDI 5200.MM applies SCRM practices piloted within the MILDEPS across the entire Department. DoD is in the process of establishing SCRM Focal Points in each of the Defense Agencies.

Although DoD has begun to institutionalize the strategies and lessons learned of from its earlier studies and FY09/10 pilot activities, it is very early in the journey toward full operational capability as required by Policy. Its current procedures will ensure that supply chain risk will be identified. However, many of the techniques for mitigating risk are difficult for programs to implement, and some are the subject of active research and development.[55]

[55] Ibid., 10.

IV. Private Sector, Security Best Practices, and Models

How do industry and other USG agencies address supply chain security risk management? In this section of the report, we discuss how the private sector views supply chain security, and what models and best practices it deploys to better manage security risks.

In the private sector, most organizations do not have a formal capability for quantifying, anticipating and mitigating/ minimizing risk. Instead, their risk management strategies or "continuity of operations plans" focus on major disruptions and specific assets, such as backup data centers or offsite data storage facilities. In effect, they are "asset-resilient" but not "mission resilient." In addition, few entities have evaluated the risks associated with new operating models, such as increased global interdependencies; expanded outsourcing relationships; and new mergers, acquisitions and partnerships.[56]

Emphasizing Symptoms vs. Scenarios

The guiding force behind any company's risk management and mitigation program, says Accenture, is preparation: understanding what potential disruptions exist; the likelihood, severity and duration of their occurrence; and the range of prioritized responses. "However, optimal preparation is not contingent on micro-identifications of every possible scenario," the report notes. "The complexities of today's environments make it nearly impossible to accurately identify all of the scenarios that might occur. A better and more practical course is to focus on commonalities across scenarios—shared symptoms. This means developing resilience frameworks not for work stoppages, hurricanes, terrorist attacks and so forth, but rather for labor shortages, destruction of property, supply disruptions and service outages."[57]

"Building a risk program around symptoms (the effects) rather than scenarios (the causes) makes resilience development manageable because it acknowledges that many events share characteristics, impacts and, most importantly, responses. There simply are too many potential disruptions for a business to develop comprehensive resilience programs for everyone."[58]

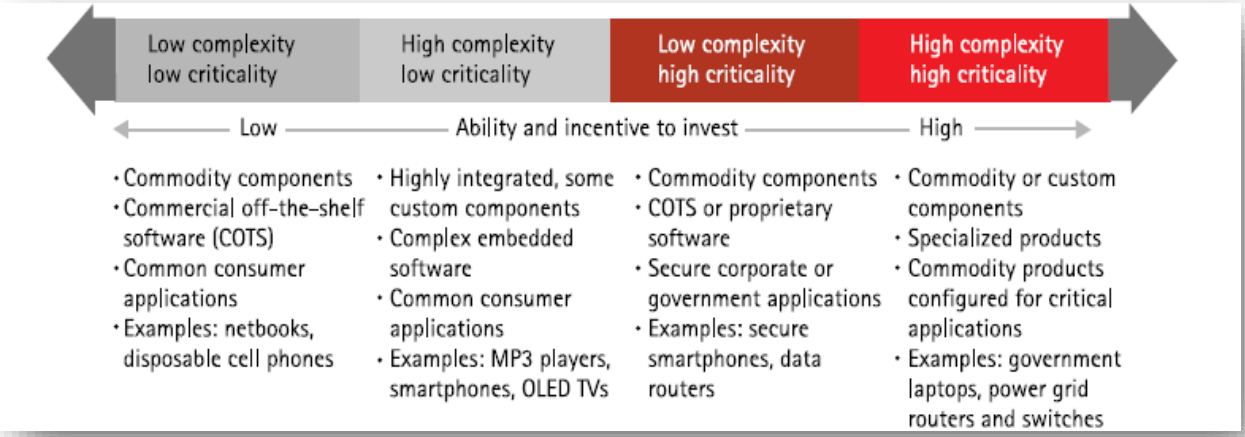
Complexity-Criticality Model

Many companies face the challenge of supporting supply chain security across the breadth of markets they serve, from low margin consumer goods to highly complex tools for business, government and critical infrastructure. As a result, these companies take a structured approach to supply chain security based on the consideration of a product's complexity and criticality. Such

[56] Accenture. "Keeping Ahead of Supply Chain Risk and Uncertainty." 2008, 4. Available at http://www.oracle.com/us/products/applications/accenture-oracle-risk-pov-bwp-069959.pdf.
[57] Ibid.
[58] Ibid.

an approach can help them select the appropriate level and type of investment in supply chain security.[59]

Figure 12: The Product Complexity - Criticality Continuum



Source: Gottlieb, Craig, "Securing Goods Across the Supply Chain: Closing the Gaps in the Manufacturing Supply Chain to Achieve High Performance." Accenture, 2010, 6. Accessed September 17, 2012. Available at http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Securing_Goods_Across_the_Supply_Chain.pdf.

In a recent report, Accenture describes this weighted complexity-criticality model as applied to the high tech sector. As Figure 12 shows, decisions about where and how much to invest become based on where each product or product family in a company's portfolio sits on the continuum of complexity and criticality. The complexity of a product is a reflection of the investment in hardware and software, ranging from commodity components such as transistors to highly customized or proprietary components and software.[60]

Criticality represents the potential impact that a counterfeit or poor quality component or product could have on the end use for which it is designed—from a minor inconvenience to a national threat. Low complexity products are those that are relatively simple to manufacture. They have a limited number of largely commodity parts in their bills of material and require a limited or less complicated logistics and manufacturing infrastructure to support their transformation from raw materials to finished goods on the shelf.[61]

[59] Gottlieb, Craig, "Securing Goods Across the Supply Chain: Closing the Gaps in the Manufacturing Supply Chain to Achieve High Performance." Accenture, 2010, 6. Accessed September 17, 2012. Available at http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Securing_Goods_Across_the_Supply_Chain.pdf.

[60]: Gottlieb, Craig, "Securing Goods Across the Supply Chain: Closing the Gaps in the Manufacturing Supply Chain to Achieve High Performance." Accenture, 2010, 6. Accessed September 17, 2012. Available at http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Securing_Goods_Across_the_Supply_Chain.pdf.

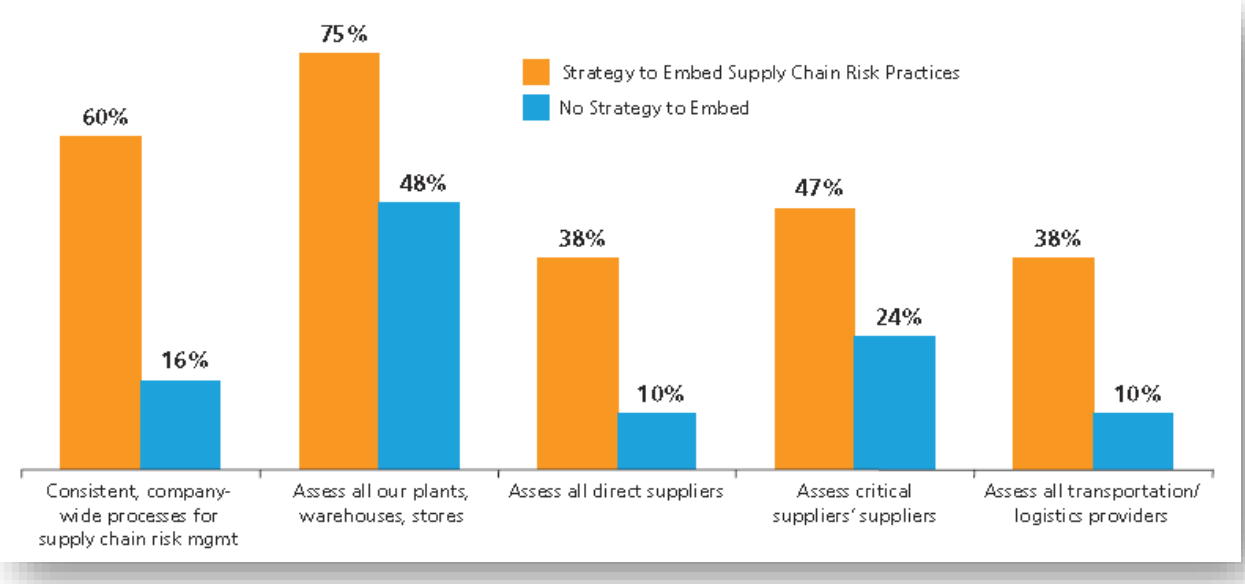
[61] Ibid.

Broaden Involvement

Companies find that broadening risk management to include suppliers as well as cross-functional teams improves results. According to Marsh research, innovator companies are nearly three times more likely to include all their direct suppliers in their risk assessments than are trailers, and twice as likely to include all their transportation carriers and logistics service providers.

Innovators are also nearly three times more likely to mobilize the company to run supply chain risk drills and tabletop exercises that span multiple departments and locations. According to study participants, cross-functional teams create the organizational alignment required for process consistency. This leads to higher rates of risk assessment both internally and externally.[62]

Figure 13: Embedding Supply Chain Risk Practices Improves Risk Assessment



Source: Enslow, Beth, "Stemming the Rising Tide of Supply Chain Risks: How Risk Managers' Roles and Are Changing Responsibilities." Report by MARSH, April 15, 2008. Available at http://usa.marsh.com/Portals/9/Documents/Stemming-the-Tide_final_4-16-08.pdf.

Rather than create separate risk processes and responsibilities, many of the most successful companies in the study have chosen to embed risk management activities and responsibilities into existing supply chain processes and functions. Organizations taking the embedding approach are much more successful in instituting end-to-end risk assessments and more consistent processes (Figure 13). This approach is not only effective, but also highly practical, given the limited resources of most corporate risk departments.[63]

[62] Enslow, Beth, "Stemming the Rising Tide of Supply Chain Risks: How Risk Managers' Roles and Are Changing Responsibilities." Report by MARSH, April 15, 2008, 9-10. Available at http://usa.marsh.com/Portals/9/Documents/Stemming-the-Tide_final_4-16-08.pdf.
[63] Ibid., 14.

Participants with risk analytics capabilities experienced dramatically lower supply chain risk impacts than their peers. Risk analytics were defined for the purposes of this study as the ability for a company to summarize total supply chain risk levels by country, supplier, or product.[64]

A Risk Management Approach[65]

To prioritize and address risks, best practice private sector organizations identify criteria for determining what may pose a risk to their operations. One potential starting point is the supply chains for the products most affecting profitability.

Using the risk criteria, the firm then identifies potential risks for key products. These may include external risks such as natural disasters, accidents, sabotage, or labor uncertainty; supplier risks such as production problems, financial issues, or subcontractor problems; distribution risks such as cargo damage, warehouse inadequacies, or supply pipeline constrictions; and internal risks such as personnel availability or facility unavailability. This process also involves prioritizing risks by the threat (as measured by likelihood and consequence) they pose to a firm's operations.

Using the prioritized risk list, the company then develops risk treatment plans. These plans include measures to protect the supply chain from risks, plans to respond to events that these risks may cause, and plans to continue operations in the face of disruptions and fully recovering from them.

The Risk Register[66]

The Supply Chain Risk Leadership Council recommends developing a "risk register", which is a one-time effort that identifies baseline risks. "Too many organizations start a risk management program without knowing what threats the organization faces, or what consequence a disruption would have, says the Council. "As a result, they focus too much on protecting against the wrong threats or too little on protecting against threats that matter. Worse, they may fail to anticipate important threats, or fail to recognize the consequence an apparently minor threat may have."[67]

A business-impact analysis helps the organization evaluate the threats it may face and their consequences. Such analysis might start with a "worst-case" scenario focusing on the business process that are most critical to recover and how they might be recovered remotely. A business-impact analysis identifies critical business functions and assigns a level of importance to each function based on the operational or financial consequence. It also sets recovery-time objectives

[64] Ibid., 15.
[65] Supply Chain Risk Leadership Council. "Supply Chain Risk Management: A Compilation of Best Practices." August 2011, 5. Accessed September 13, 2012. Available at http://www.scrlc.com/articles/Supply_Chain_Risk_Management_A_Compilation_of_Best_Practices_final[1].pdf.
[66] Ibid., 12.
[67] Ibid.

and the resources required for these. Figure 14 presents examples of threats a commercial organization may wish to consider for mitigation.

Figure 14: Potential Risks to an Organization and its Supply Chain

	Natural Disasters	Accidents
External, End-to-End Risks	Sabotage, terrorism, crime, war	Political uncertainty
	Labor unavailability	Market challenges
	Lawsuits	Technological trends
Supplier Risks	Physical and regulatory risks	Production problems
	Financial losses and premiums	Management risks
	Upstream supply risks	
Distribution Risks	Infrastructure unavailability	Lack of capacity
	Labor unavailability	Cargo damage or theft
	Warehouse inadequacies	IT system inadequacies or failure
	Long, multi-party supply pipelines	
Internal Enterprise Risks	Operational	Political uncertainty
	Demand variability	Personnel availability
	Design uncertainty	Planning failures
	Financial uncertainty	Facility unavailability
	Testing unavailability	Enterprise underperformance
	Supplier relationship management	

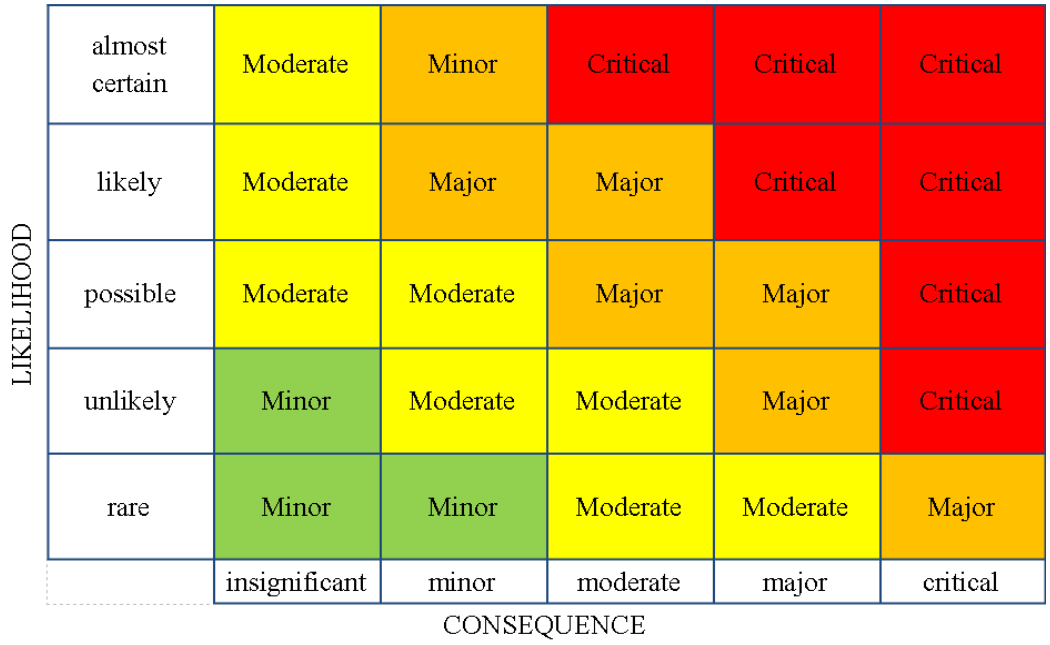
Source: Supply Chain Risk Leadership Council. "Supply Chain Risk Management: A compilation of best practices." August 2011, 12-13. Accessed September 13, 2012. Available at http://www.scrlc.com/articles/Supply_Chain_Risk_Management_A_Compilation_of_Best_Practices_final[1].pdf.

The risk analysis process estimates the likelihood and consequence of risks facing a firm and accordingly prioritizes them for ultimate treatment. To begin, firms may choose to rank risk events based on a qualitative overall risk level. "Such a simplistic approach should only be used for the initial risk register, but provides an easy way to quickly prioritize perceived risks and select those that should receive priority attention," advises the Supply Chain Risk Leadership Council.

Another means of evaluating risk is to use a "heat-map" showing risk-events on a matrix defining likelihood and consequence levels. As the Supply Chain Risk Leadership Council explains, this technique allows managers to easily see the relative likelihood and consequence of differing risks. To use this method effectively it is critical to have well-defined and consistently

used criteria for the different likelihood and consequence levels. Figure 15 shows a heat-map illustrating the concept.

Figure 15: Heat Map of Risk Events Matrix



Source: Supply Chain Risk Leadership Council. "Supply Chain Risk Management: A compilation of best practices." August 2011, 18. Accessed September 13, 2012. Available at http://www.scrlc.com/articles/Supply_Chain_Risk_Management_A_Compilation_of_Best_Practices_final[1].pdf.

The Pharmaceutical Industry's Approach to Supply Chain Security

The pharmaceutical industry faces many of the same supply chain security challenges as DoD – with results/impacts that range from inconvenience to death. And like DoD, adulteration, counterfeiting, and illegal diversions are major issues for pharmaceutical firms.

Quality systems alone cannot ensure supply chain security or security. However, as a recent report from the International Society for Pharmaceutical Engineering (ISPE) advises, "Augmenting specific quality systems, being alert to signals in the environment, applying risk management principles, and developing specific programs to deal with counterfeiting and illegal diversion can strengthen an organization's overall supply chain security."[68]

The World Health Organization defines counterfeit medicines as follows:

> *"A counterfeit medicine is one which is deliberately or fraudulently mislabeled with respect to identify and/or source. Counterfeiting can apply to both branded or generic*

[68] ISPE: International Leadership Forum. "Supply Chain Security: A Comprehensive and Practical Approach." Tampa, Florida. 2010, 5.

products and counterfeit products may include products with the correct ingredients or with the wrong ingredients, with insufficient active ingredients or fake packaging."[69]

A pharmaceutical manufacturer may not be able to fully prevent counterfeiting across the global marketplace. The goal is to define appropriate controls to minimize the risk of counterfeit product.

Pharmaceutical companies perform risk assessments to help identify which products and regions present the greatest risk of counterfeiting. They use these assessments to help prioritize the allocation of anti–counterfeiting resources.[70]

The sector employs several common tools to help control the risk of adulteration, counterfeiting, theft and illegal diversion. These include:[71]

- Signal detection and response
- Supplier quality management, and
- Selection and management of logistics/transportation service providers.

Signal detection and response as the ITE study explains, "is a signal of new information indicating the potential for economically motivated adulteration of a material or a product, the use of counterfeit material, or the diversion of legitimate product into lawful channels. Often, a signal consists of information related to a change in the availability or price of a material or product, or it can be a precursor event likely to lead to such a change. The change may create an incentive to substitute alternative material for legitimate material into lawful channels."[72] For example, if the cost of a key ingredient skyrockets, unethical companies may opt for illegal ingredients substitution.

As the ISPE outlines, the signal detection process involves

1. Defining targets for enhanced, ongoing scrutiny
2. Applying environmental scanning for signals to identify targets (reviewing external information that may have an impact on the targets)
3. Determining the relevance of the results of the environmental scans.

Supplier quality management, which strives to reduce risk by thoroughly vetting supplier quality track record and processes, has three key elements:[73]

- Supplier assessment and selection
- Written agreement for quality activities
- Supplier monitoring and review.

[69] Ibid.
[70] Ibid.
[71] Ibid., 11.
[72] Ibid.
[73] Ibid., 15.

Supplier assessment and selection apply quality risk management principles to the process of assessing and selecting a potential supplier. The approach should be appropriate to the material being supplied – e.g., the approach to assessing and selecting a potential drug product supplier will be more extensive than that of choosing a packaging supplier. The assessment also may differ based on geographic location of the supplier and the regulatory environment under which the supplier operates.

Requirements and standards are clearly documented and communicated to the supplier at the start of the assessment/selection process. This allows suppliers to access their capability and willingness to meet these expectations.

For all new suppliers, the ISPE recommends assessing whether an on-site audit is warranted as part of the selection process. "The scope, duration, number of auditors, depth, and content of the audit should be risk based," ISPE advises, "for example, where there is a risk of economically motivated adulteration or when assessing suppliers in regions where the regulatory framework is still developing, a special approach to the audit may be required to assess additional risks such as fraud, illegal diversion, and counterfeiting.[74]

"The full extent of the supply chain should be known and documented," the organization continues. ISPE recommends gathering current information from second- and third-tier suppliers regarding the supply chain from the origin of procured materials through to receipt at the manufacturing location.[75]

Any deficiency found as part of the supplier assessment should be rated as to seriousness and timing for remediation.

Once the prospective supplier assessments are completed, ISPE recommends that pharmaceutical manufacturers conduct a formal risk assessment to capture the risks identified during the evaluation and any risk controls required. This assessment should include quality, regulatory, technical and performance strategies to reduce and/or mitigate identified risks. It should capture costs relating to risk mitigation. This assessment is an important aid in supporting the decision to select or reject a vendor/supplier.[76]

Supplier performance should be monitored and reviewed on a regular basis. ISPE advises, "There should be a process to monitor performance across the supply chain. This starts with the complete understanding of the supply chain. Ongoing verifications of the effectiveness of an organization's supplier's quality systems to manage suppliers and supply chain is important. This can be accomplished through targeted auditing of these quality systems. There should be a periodic verification of the chain of custody."[77]

[74] Ibid.
[75] Ibid.
[76] Ibid.
[77] Ibid., 17.

Other pharmaceutical industry best practices for security include the following:[78]

- Physical security of facility
- Procedures for handling and destruction of waste, particularly rejected product and packaging components.
- Procedures for the secure handling and storage of the product security features such as tamper evident labels, holograms, and other components including packaging materials
- Procedure for the secure storage and control of product security specifications and manufacturing formulas
- Adherence to company and/or site specific procedures for the handling of suspected counterfeit events
- Review of production yields, capacity, and/or product amounts compared with raw material purchases
- Training and qualification of personnel directly involved in product security and counterfeit detection.
- Well-defined logistics and transportation security systems and controls.

ISO 28002: 2011

ISO has developed a new standard, **ISO 28002:2011*, Security management systems for the supply chain – Development of resilience in the supply chain – Requirements with guidance for use***. ISO 28002 offers a comprehensive and systematic process to enhance prevention, protection, preparedness, mitigation, response, continuity of operations and recovery from disruptive incidents. Its generic auditable criteria, when implemented in a management system, can be used to establish, implement, monitor, review, maintain and improve an organization's resiliency policy to plan for, take action and make decisions before, during and after an incident to its supply chain.

Source: Proctor, Paul E and Smith, Michael, "The Gartner Business Risk Model: A Framework for Integrating Risk And Performance." September 1, 2011.

Selection and management of logistics/transportation service providers[79] involves applying the same principles used in supplier selection. Inspecting physical facilities and transportation equipment, assessing security measures and processes are necessary parts of a security assessment. Financial soundness, capability of meeting contractual security requirements, and the ability to identify and correct security deficiencies also require review.

ISPE advises that background information including a history of claims, the types of commodities handled, and the geographic areas served should be supplied by the service providers and used as part of the assessment and selection process. Hiring practices of the provider should be reviewed.

[78] Ibid.
[79] ISPE: International Leadership Forum. "Supply Chain Security: A Comprehensive and Practical Approach." Tampa, Florida. 2010.

A review of the relevant permits will also demonstrate if the provider is authorized to handle pharmaceutical products where such permits are required. If the provider will be handling controlled substance, those permits should be reviewed along with necessary security measures such as caged areas.

V. Case Studies and Examples

In this section of our report, we present several case studies and discussion examples relating to supply chain security. These cases include:

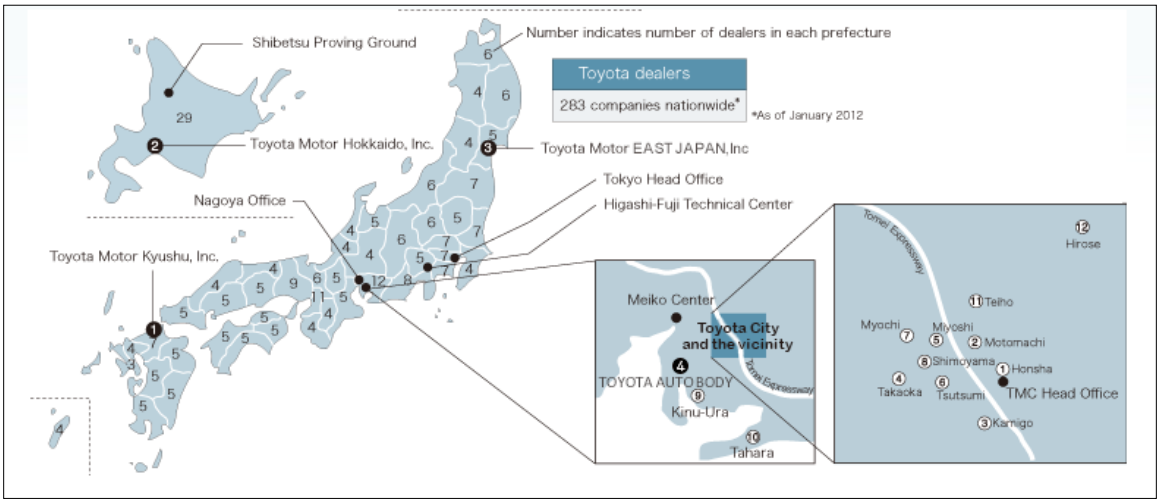
- Toyota Motors Corp.: The supply chain impact of the 2011 earthquake and tsunami
- CISCO
- McAfee: Securing the information supply chain
- NASA

Case #1: Toyota Motors Corp.

How the 2011 Earthquake-Tsunami Impacted Toyota's Supply Chain

On March 14, 2011 Japan's pacific coast of Tohoku was hit by a massive earthquake. The earthquake triggered a powerful tsunami which in turn caused extensive damage resulting in a near nuclear meltdown at a reactor site. The earthquake-tsunami-nuclear shutdown was a disaster for many industries, including automotive. Nearly 38 percent of cars sold worldwide are produced in Japan, including Honda, Nissan, Toyota, and GM.

Figure 16: Locations of Toyota Facilities as of December 2011



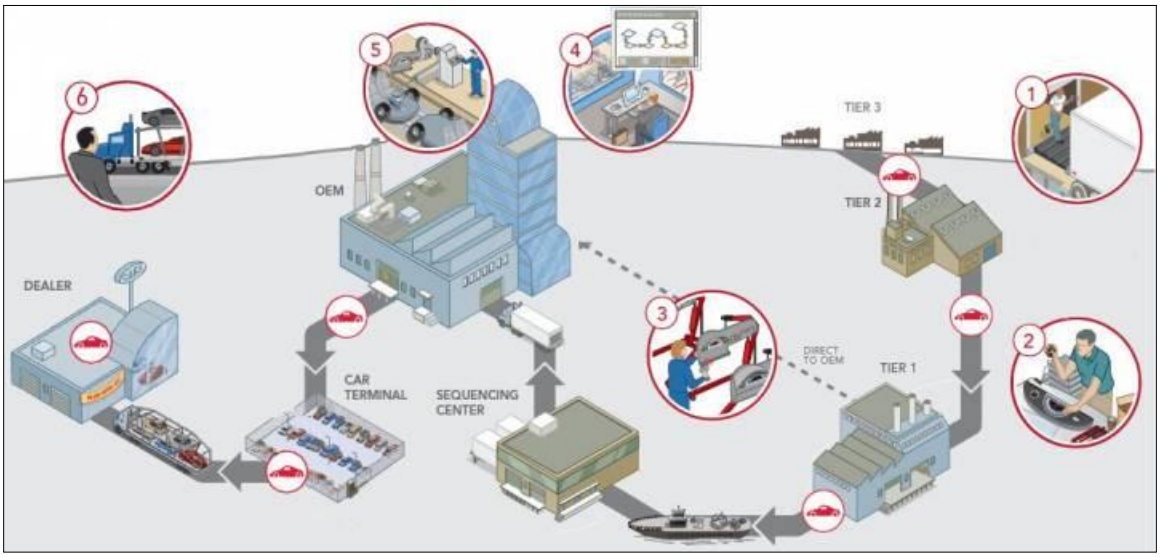
Source: Toyota. "Worldwide Operations." Accessed September 24, 2012 http://www.toyota-global.com/company/profile/overview/in_the_world/.

Toyota maintained 12 plants and 4 manufacturing sites in Japan (an additional 50 manufacturing sites were located outside Japan)[80]. This earthquake disrupted Toyota's entire supply chain in Japan, halting the production at all 12[81] assembly plants. Figure 16 pinpoints Toyota's facilities in Japan. Initially, all of Toyota's operations were shutdown from March 11th till March 22nd. Toyota was able to ship parts but not cars after March 21st. Damage to the electrical grid,

[80] Toyota. "Worldwide Operations." Accessed September 24, 2012 http://www.toyota-global.com/company/profile/overview/in_the_world/.
[81] Refer Appendix

transportation networks, and ports limited Toyota's capability to sell many new cars, in particular almost the entire Lexus product line. (Figure 17 shows the basic flow structure of Toyota's supply chain.) Figure 18 identifies Toyota's financial losses.

Figure 17: Structure/Supply Chain of Toyota

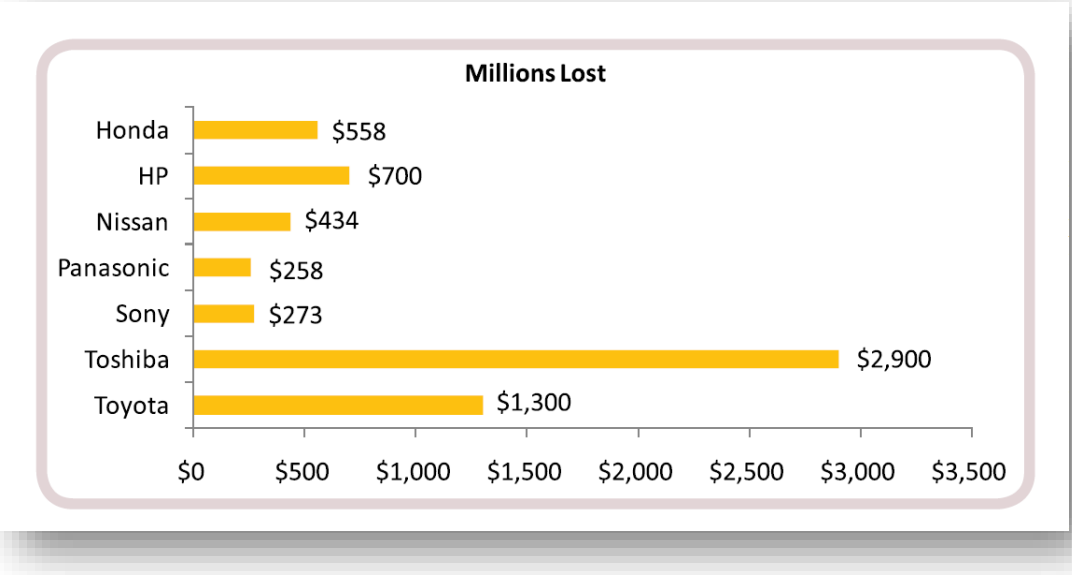


Source: Toyota Motor Corporation. Accessed September 24, 2012
http://chawalit.siit.tu.ac.th/doku.php?id=seniorprojects:2009:report_marvellous:toyota_motor_corporation.

The disaster uncovered a major flaw in Toyota's supply chain and, more broadly, in its operating strategy. While highly cost efficient and lean, the supply was also high risk. For example, 40 percent of computer chips used to power Toyota's vehicles were supplied solely by Renesas using a six-minute JIT supply method. This required months to replace the lost capacity, a delay that cost Toyota market-share and its number one position as global sales leader.[82]

[82] Schreffler, Roger. "Quake Changes Little in Toyota's Supply Chain Strategy." Wards Auto. Last modified May 16, 2012. Accessed September 24, 2012 http://wardsauto.com/supply-chain/quake-changes-little-toyota-s-supply-chain-strategy-0.

Figure 18: Earthquake Losses of Sample Electronics and Automotive Companies as of May 2011



Source: Brennan, Patrick. "Lessons Learned from the Japan Earthquake." *Disaster Recovery Journal* Summer 2011: 22-26. Accessed September 27, 2012 http://www.supplyrisk.com/Lessons_Learned_from_the_Japan_Earthquake.pdf.

Although Toyota's production was severely hampered by the earthquake with 300 suppliers reporting facility damages[83], the company expected to return to the same level of production as before the earthquake by the end of July 2011 and full production by November/December 2011. Toyota's production in Japan fell 63.1 percent in March 2011 alone[84] with output through June 2011 delayed by approximately 760,000 vehicles globally compared to 2010.[85] Toyota planned to produce 350,000 additional vehicles from October to March to make up for production lost in the disaster.[86]

Toyota was able to restore the supply network and recover output of about 600,000 units from July on with overtime production. The total impact in fiscal 2012 was decreased output of about 150,000 vehicles. Domestic Japanese production returned to almost normal levels by July 2011 and was fully restored by September 2011.[87]

In October-November 2011, severe flooding in Thailand interrupted Toyota's supply chain again. Approximately 100 components solely manufactured in Thailand were unavailable,

[83] Ibid.
[84] Schmitt, Bertel. "Toyota Data Production Hit Hard in March." Last modified April 25, 2011. Accessed September 27, 2012 http://www.thetruthaboutcars.com/2011/04/toyota-production-data-hit-hard-in-march/.
[85] Toyota Motor Corporation Annual Report. 2012, 30. Accessed September 24, 2012 http://www.toyota-global.com/investors/ir_library/annual/pdf/2012/
[86] Smith, Aaron. "Toyota's Woes: Lower Sales, Ratings Cut." *CNN Money*, last modified June 28, 2011 http://money.cnn.com/2011/06/28/news/international/toyota_earthquake/index.htm.
[87] Toyota Motor Corporation Annual Report. 2012, 30. Accessed September 24, 2012 http://www.toyota-global.com/investors/ir_library/annual/pdf/2012/

causing cutbacks in overtime of other Toyota plants in Japan, North America, and Africa. Thailand floods caused a decreased output of about 240,000 vehicles in fiscal 2012.[88]

The Solution

Although Toyota was recognized for its supply chain management and pioneering in lean production, the company was surprised by the ripple effect, these disasters caused in the industry. According to Toyota's Executive Vice President Shinichi Sasaki, "Our assumption that we had a total grip on our supply chain proved to be an illusion."[89]

In Toyota's annual report for FY April 2011-March 2012, the company reported conducting a "visualization" analysis of the supply chain, including mapping out the locations and products of primary suppliers and availability of supplies from third and fourth-tier suppliers through to primary suppliers. The visualization showed that among 1,500 supplier sites, 300 were "at-risk" locations, representing the sole sources for almost 1,000 parts. Toyota asked these suppliers to spread production or hold extra inventory. Toyota provided restoration support for suppliers visited during the investigation process and looked for substitute products if restoration was problematic.

In May 2012 Toyota came up with a strategy to make its supply chain more resilient, including a two-week recovery plan. Sasaki said the three-step process to reduce supply chain risks would be completed in about five years: [90][91][92]

1) Standardization of parts/consolidation for suppliers: Create common parts that can be shared among manufacturers in several locations and can be substituted between models of vehicles to reduce inventory and risk. This may also make it financially reasonable for a supplier to manufacture the parts in multiple locations because the demand for common parts would increase significantly.
2) Holding inventory and developing technology: (Part I) Ask suppliers to maintain a few months' worth of inventory for specialized components that cannot be built in multiple locations rather than relying on JIT inventory method. (Part II) Develop technology so alternatives remain available for parts and materials. If the supply of one material is cut off or used up, then an alternative material has already been researched and developed and available immediately.

---

[88] Ibid.
[89] SCDigest Editorial Staff. "Global Supply Chain News: Toyota Taking Massive Effort to Reduce its Supply Chain Risk in Japan." *Supply Chain Digest*. Last modified March 7, 2012. Accessed September 27, 2012 http://www.scdigest.com/ontarget/12-03-07-2.php?cid=5576&ctype=content.
[90] Allianz Global Corporate & Specialty. "Global Supply Chains: The Growing Risks of Business and Supply Chain Interruption in Today's Interconnected World." March 2012. Accessed August 29, 2012 http://www.agcs.allianz.com/assets/PDFs/Special%20and%20stand-alone%20articles/Supply_Chain_Factsheet.pdf.
[91] Kim, Chang-Ran. "Toyota Aims for Quake-Proof Supply Chain." *Reuters*. Last modified September 6, 2011. Accessed September 27, 2012 http://www.reuters.com/article/2011/09/06/us-toyota-idUSTRE7852RF20110906.
[92] SCDigest Editorial Staff. "Global Supply Chain News: Toyota Taking Massive Effort to Reduce its Supply Chain Risk in Japan." *Supply Chain Digest*. Last modified March 7, 2012. Accessed September 27, 2012 http://www.scdigest.com/ontarget/12-03-07-2.php?cid=5576&ctype=content.

3) Region dependency: Each region should independently obtain its parts to prevent one region's disaster from affecting the rest of the regions. For example, North American production would not rely on the same set of suppliers on which Japanese production relies. Additionally, this method eventually lowers costs by placing costs and revenues in the same currency, thereby eliminating losses related to foreign exchange rates.

Results

Toyota's previously gold standard supply chain management strategy of lean production was caught off guard by the earthquake, tsunami, and floods. Too late, Toyota realized needed improvements in transparency and knowledge of its entire supply chain.

Toyota did not know where all tiers of its supplier factories were located, leaving it completely blind and unable to fully assess the situation post-quake. After completing the visualization analysis, Toyota has a complete understanding of each supplier down to the third and fourth tiers. ''We thought our supply chain was pyramid shaped, but it turned out to be barrel-shaped,'' said a Toyota Motor Corporation spokesman in a recent Japan Times article. Before the earthquake, Toyota maintained single suppliers for many products required for its vehicles. Toyota continues to need to increase not only the number of sources but also the distribution of sources. In the tsunami disaster, for example, two semiconductor suppliers that provided 25 percent of the global supply of silicon wafers used in semiconductors were knocked out, resulting in production shortages for Toyota. Diversifying the supplier bas geographically would prevent this problem.[93]

Toyota reports it is increasing dual- and triple-sourcing of strategic components and materials both in and outside of Japan. However, diversifying sourcing may reduce short-term profits, the company acknowledges.[94]

Case #2: CISCO

Global Supply Chain Risk Management

Cisco's supply chain risk management (SCRM) program is widely regarded as one of the best in the industry. It not only secures the supply chain, but builds resiliency into the company's global business – a resiliency that translates into competitive advantage. This case study describes CISCO's SCRM effort in detail.

[93] Brennan, Patrick. "Lessons Learned from the Japan Earthquake." *Disaster Recovery Journal* Summer 2011: 22-26. Accessed September 27, 2012 http://www.supplyrisk.com/Lessons_Learned_from_the_Japan_Earthquake.pdf.
[94] Schreffler, Roger. "Quake Changes Little in Toyota's Supply Chain Strategy." Wards Auto. Last modified May 16, 2012. Accessed September 24, 2012 http://wardsauto.com/supply-chain/quake-changes-little-toyota-s-supply-chain-strategy-0.

"You simply cannot predict what type of disruptions your supply chain will encounter."

"In 2005, we thought we could – so we took an actuarial approach to finding hot spots in the world. But we realized that the fundamental dynamic of our business is that our company will never move our sources of supply and manufacturing simply because of risk. And we can never predict which of the five horsemen will strike and when.

"So we said, 'Let's not try to predict. Let's build a process and set of tools - and build credibility within the company for those processes and tools - so that we can pull the right resources, tools, processes, and management support together at a moment's notice to manage any crisis that comes up. And do this in a repeatable, scalable manner."

That's how James Steele, Director of Supply Chain Risk Management at Cisco described the genesis of the networking company's SCRM effort in a recent presentation.[95] "Since its inception in 2006, our program has evolved based on working through actual crises," Steele noted. "We've had 65 crises since I've been leading the team, ranging in size from small to large. We used them as key learning opportunities."

Program Overview

CISCO's approach to supply chain risk management is based on a balance between readiness and proactive resilience, Steele explains. The SCRM program combines tools, policies, practices and management support into a comprehensive system that enables the company to understand and manage the risks associated with the product supply. Beginning with new product design and introduction, and continuing through to current product manufacturing and fulfillment, Cisco can predict potential risk points and work with members of its supply chain to manage and minimize those risks. Further, Cisco can recover from external disruptions quickly to minimize the impact on its customers.[96]

Cisco relies extensively on outsourced manufacturing for more than 95 percent of its 12,000-plus products, most of which are configure-to-order. The company sells to a broad range of customers in the private and public sector.[97]

From a high-level view, the threats to a company's business can be divided into external and internal risks. Internal risks may be further divided into three subcategories: strategic, operational and financial risks.[98]

- **External risks** include events such as economic downturns, pandemics, natural and man-made catastrophes, acts of war and terrorism, political turmoil and regulatory concerns.
- **Internal strategic risks** involve threats to the company's business model, product or service portfolio, brands, reputation and standing in the marketplace.

[95] James Steele, Cisco, presentation, Annual Global Conference, Council of Supply Chain Management Professionals, Atlanta, September 2012.
[96] Mikovic, Dan and Roberta J. Witty. "Case Study: Cisco Addresses Supply Chain Risk Management." *Gartner*. September 17, 2010, 2.
[97] Ibid.
[98] Harrington, Lisa H, Sandor Boyson, and Thomas M. Corsi. "CISCO Case Study." *X-SCM: The New Science of X-treme Supply Chain Management*. New York: Routledge, 2011, 105.

- **Internal operational risks** are problems that can affect productivity, profit margin, the supply chain, and the physical plant, as well as employee relations and morale.
- **Internal financial risks** have to do with cash flow, equity, stock price, investments, mergers and acquisitions, foreign exchange, interest rates and other fiscal matters.

On the supply chain side, risks are inherent in all activities, including:[99]

- Sourcing
- Manufacturing
- Transportation
- Storage.

Cisco's concern about supply chain risk is not limited to natural disasters. The company seeks to manage any kind of potential disruption or volatility. "Any of the [supply chain] volatilities could translate into market opportunities or disruptions," reported John O'Connor, Director of Global Supply Chain at Cisco. "If we don't have a higher level of awareness and acknowledgement of resiliency, they will translate into disruptions." By embracing volatility management, Cisco captures "market adjacencies," expanding into new product and market opportunities.[100]

The SCRM program is designed to formalize risk management relative to business continuity planning. It works around three functional disciplines:[101]

- Business process continuity
- Crisis management
- Product and supply chain resilience.

Business Continuity Planning (BCP)[102]

BCP is a semiannual process to assess critical value chain partners. BCP's five steps include:

1. Identifying key nodes with high impact potential**.** Nodes are characterized as a location where a single-source supplier is located or as a major logistics hub or supplier that touches a large part of the product portfolio. Key nodes are defined as those with a high revenue impact potential.
2. Evaluating preparedness based on an objective format. Cisco has developed a Web-based tool that evaluates critical supply chain partners based on standardized risk criteria. The tool is used as the basis for periodic preparedness audits of these suppliers.
3. Mapping critical components to supplier sites. This web-based tool provides a geographic visualization capability for mapping critical components to supplier sites all over the world.

---

[99] Ibid., 106.
[100] Ibid, 106.
[101] DeAngelis, Stephen F,. Insights on Technology, Business and Government with a Focus on Supply Chain Management, Artificial Intelligence and Innovation blog. http://www.enterrasolutions.com/blog
[102] Mikovic, Dan and Roberta J. Witty. "Case Study: Cisco Addresses Supply Chain Risk Management." *Gartner*. September 17, 2010, 3.

4. Identifying time to recover (TTR) at the part and site levels. TTR can be measured at the manufacturing, test or component level. It can be remediated by second sourcing, recovery locations and so on. TTR is a critical element in defining resiliency in Cisco's program. Cisco validates suppliers' TTR through regular audits and test drills. If a supplier fails an audit, it may be put on a performance improvement program or see some of its volume shifted to other suppliers.

"The key to business continuity planning," observed Steele, "is to build a database of all the information we could need, so if there is an incident, we know who our secondary sources are, where they're located, whom to contact, whether they have back-up power and water, and so on. This database is the backbone of the program, and it is critical to maintain it as current."[103]

Crisis Management

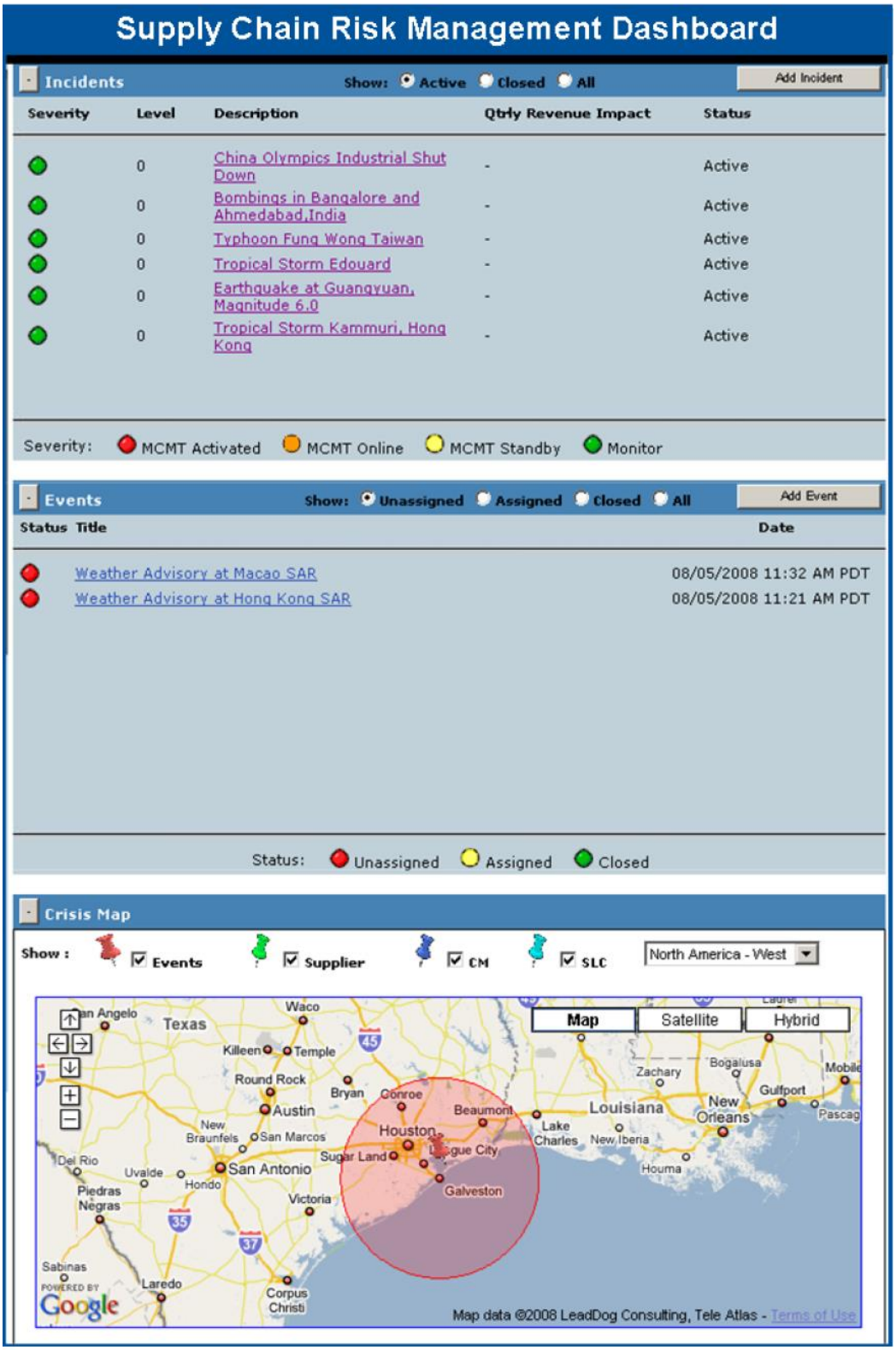
Using external situational awareness risk feeds from an external provider, NC4 (www.nc4.us), Cisco has developed a crisis management dashboard that can display potential disruptive threats on a global basis. The dashboard enables Cisco to monitor threats – potential and actual – on a real-time basis anywhere in the world (Figure 19).[104]

Product and Supply Chain Resiliency

To help it standardize and automate risk assessment, Cisco has developed a "risk engine," (software analytic tool) that incorporates many data sets (such as 100-year flood, actuarial, geological, geopolitical, site-incident and supplier performance data) to assess the likelihood of a disruption. These disruptions are correlated to Cisco's supply chain locations, including supplier sites, contract manufacturing facilities and logistics centers. The potential impact of a disruption is determined based on the revenue associated with each supply chain node and that node's TTR. Finally, Cisco uses simulation to integrate all of these data sets into a single model that forecasts the likelihood and impact of disruptions and generates "heat maps" identifying potential trouble spots.[105]

[103] Steel, James. "Cisco." Presented at the Annual Global Conference, Council of Supply Chain Management Professionals, Atlanta, GA, September 2012.
[104] Mikovic, Dan and Roberta J. Witty. "Case Study: Cisco Addresses Supply Chain Risk Management." *Gartner*. September 17, 2010, 4-5.
[105] Harrington, Lisa H, Sandor Boyson, and Thomas M. Corsi. "CISCO Case Study." *X-SCM: The New Science of X-treme Supply Chain Management*. New York: Routledge, 2011, 108.

Figure 19: Cisco's Crisis Management Dashboard



Crisis team activation

Global monitoring of events that may disrupt Cisco's supply chain

Mapping capabilities to assess supply chain nodes within the radius of an event

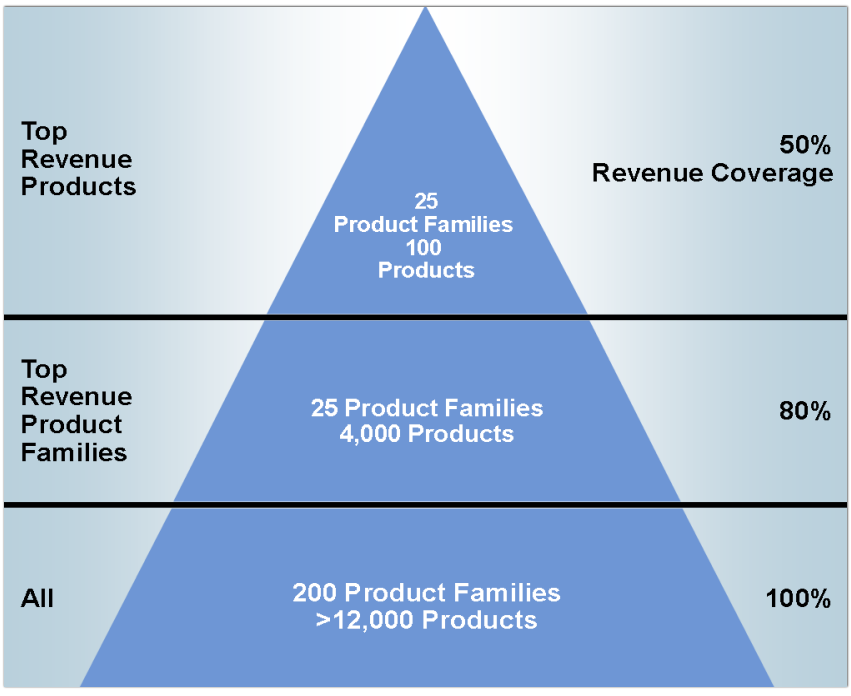
Source: Mikovic, Dan and Roberta J. Witty. "Case Study: Cisco Addresses Supply Chain Risk Management." *Gartner*. September 17, 2010, 5.

These maps identify the portfolio of assets that are at risk, the level of risk, what considerations need to be built into the business model to address the risks, and how the risks should factor into a group's or business unit's decision-making process.[106]

Cisco has developed its own method of risk probability modeling. When analysts look at the bill of materials (BOM) for a specific product, they know which suppliers are contributing componentry, which manufacturing partners are involved, and who is handling testing, and who is managing subassembly distribution. They consider which customers are buying that product as well as the transportation routing. Thanks to the regular collection and updating of data, all of that assessment can be completed in about an hour, O'Connor said.[107]

Analysts have the ability to isolate the revenue impact of a potential or actual disaster regardless of whether it affects a supplier, contract manufacturer or Cisco location. They know the products that are affected and their revenue value, as well as their recovery times. For risk management purposes, Cisco prioritizes its products based on their revenue impact, as shown in Figure 20. For example, 100 products in 25 product families represent 50 percent of Cisco's revenue; 4,000 products within 25 product families represent 80 percent of revenue.[108]

Figure 20: Cisco's Revenue Impact



It can cost as much as $1 million to de-risk an established legacy product, because of all the steps required to build in product protection after the fact. Therefore, Cisco has learned that it is more effective and less expensive to adopt a proactive approach to products, and de-risk them in the initial design phase. As a result, new products are now entering production with relatively low risk indexes.[109]

Source: Mikovic, Dan and Roberta J. Witty. "Case Study: Cisco Addresses Supply Chain Risk Management." *Gartner*. September 17, 2010.

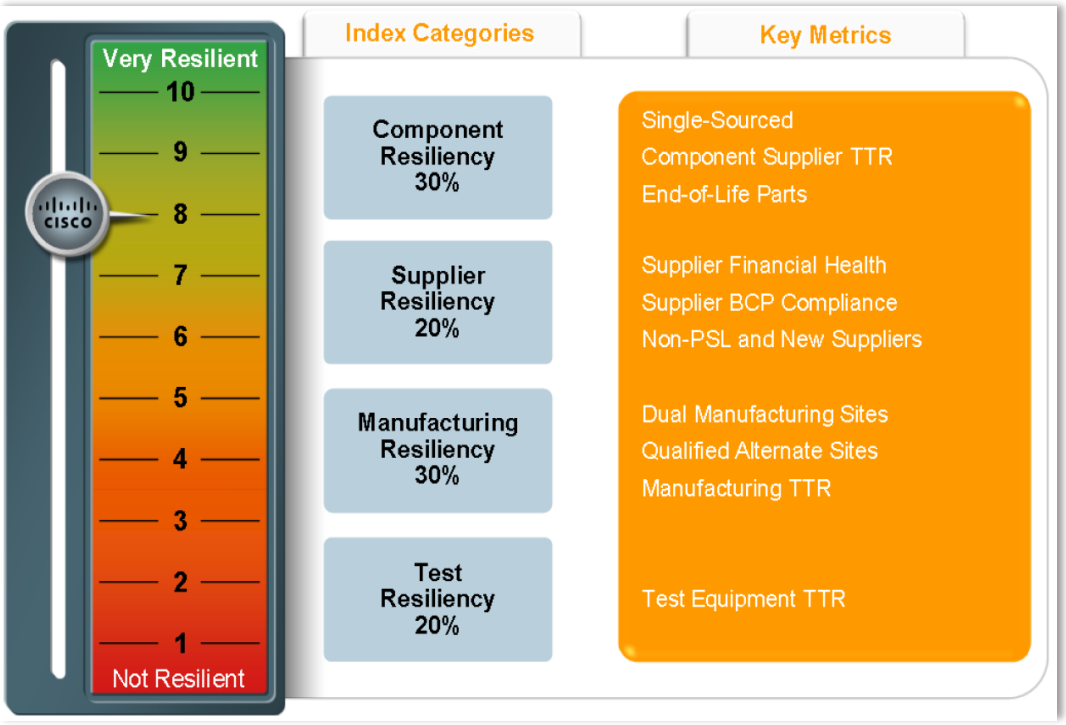
[106] Ibid.
[107] Ibid.
[108] Ibid.
[109] Mikovic, Dan and Roberta J. Witty. "Case Study: Cisco Addresses Supply Chain Risk Management." *Gartner*. September 17, 2010, 10.

Typical product de-risking steps might include[110]:

- Selecting alternative components that have multiple sources of supply
- Selecting existing components with similar and acceptable performance characteristics, instead of an all-new design
- Substituting a commodity-grade component with additional testing, instead of a premium component and vice versa — whichever has lower risk
- Qualifying additional manufacturing sites
- Specifying alternate test procedures.

To ensure the metrics were objective and comparable, Cisco created an index that is used either to judge a supplier or assess a particular product/design. The index has multiple elements. For designs/products, the component element and manufacturing and test elements are critical, while the supplier-centric metrics replace the component-based metrics for suppliers (Figure 21).

Figure 21: Cisco's Resiliency Index Definition



Source: Mikovic, Dan and Roberta J. Witty. "Case Study: Cisco Addresses Supply Chain Risk Management." *Gartner*. September 17, 2010, 6.

Institutionalizing Risk Management

Cisco has gone to great lengths to institutionalize its risk management strategy at all levels of the enterprise. Risk management is embedded at the corporate level (the CFO has a risk management

[110] Ibid.

function); within the information management system; and at the operations and product levels. All of these areas and managers must coordinate and align their risk management activities. "We have been working on an enterprise governance model that will have risk and resiliency sponsor groups that work at various levels," explained O'Connor. These include the Risk and Resiliency Operating Committee and several working groups focused on Business Continuity Management, Pandemic Planning, Crisis Management and Risk Governance and Metrics. "The working groups help us understand how to manage risk and measure our operating level relative to our risk appetite," O'Connor added.[111]

Cisco has a formal risk portfolio management process to manage how it allocates funding to mitigate risks within the supply chain. The process organized in three phases, proceeding in chronological order:[112]

1. **Program Scope**: Determine which products the team will consider as candidates for risk mitigation. The strategic focus for the team is the highest revenue products for Cisco
2. **Budget Approval Process**: Supplier management teams submit mitigation funding requests which are then allocated based on revenue impact and available budget
3. **Pipeline Process**: Rank projects based on product revenue ranking; schedule projects for the fiscal year with expense and capital identified by quarter; review quarterly projects to ensure full utilization of SCRM budget
4. **Project Management Process**: Develop project plans with milestones until the mitigation actions are closed; track and report monthly progress against milestones; release scheduled payments or re-direct funds to next-in-line.

Preparing For and Responding to a Crisis

Crisis management at Cisco consists of four components: global event monitoring, continuity planning, impact analysis, and response playbooks. Potential disruptions in the supply chain including events at key manufacturing and commodity supplier sites as well as business-critical infrastructure sites, such as airports, are monitored by the Supply Chain Risk Management (SCRM) team using a worldwide alert service.

Cisco's SCRM team also categorizes risk exposure for impact by:

- Type of risk ranked by location (e.g., weather or natural disaster)
- Type of risk ranked by product revenue category (e.g., 100 products represent 50 percent of Cisco's revenue at risk)

Cisco often uses maps and graphic representations to indicate the location and degree of supply chain risk. Cisco's Supply Chain Risk Management team diagrams the projected impact of

[111] Harrington, Lisa H, Sandor Boyson, and Thomas M. Corsi. "CISCO Case Study." *X-SCM: The New Science of X-treme Supply Chain Management*. New York: Routledge, 2011, 109.
[112] Ibid., 109-110.

natural disasters, such as earthquakes or typhoons, on strategic locations. On a map of the world, for instance, there are red (extreme risk), orange (severe) and yellow (moderate) dots of different sizes. This shows relative risk based on the number of locations (including: supplier, manufacturing, transportation and logistics), the likelihood of a disruption and the potential impact of a disruption. Zooming in closer to geographic regions, Cisco can view supply chain risk locations in more detail.[113]

Cisco leverages the data collected via the BCP program to build maps of its supply chain and graphic representations to indicate the location and degree of supply chain risk. For a specific event or risk, the team can highlight a region of concern and quickly identify any critical sites within that region. This allows the team to quickly identify locations impacted by an event such as an earthquake, flood or strike and determine the potential revenue impact. Analysts can clicking each site on the map and get details about the company, emergency contacts, revenue impact, time to recover, and an alternate source of supply or services.[114]

When the Chengdu earthquake hit in 2008, Cisco's supply chain risk analysts had a wealth of information at their fingertips. Marrying previously collected data about products and revenue exposure with current reports of damage allowed them to quickly assess the impact on other supply chain nodes and on customers. On a satellite map of China, the team could quickly identify any manufacturing sites, logistics centers and supplier locations that could potentially be affected by the earthquake and the disruptions it could cause in the immediate vicinity as well as in Shanghai, Hong Kong, Guangdong, Macau, and other areas in the eastern half of the country. As it turned out, four suppliers of four products were located within the earthquake zone and were moderately affected. The analysts were able to quickly determine those suppliers' anticipated time to recover and the estimated revenue impact of lost capacity during that period.[115]

When a problem does occur, Cisco's supply chain incident management team is ready to go. Aided by both a supply chain monitoring capability and a defined set of protocols, the team can quickly respond to events that may impact the supply chain in addition to leveraging predefined ways to communicate with the entire organization. In order to monitor the supply chain, Cisco identified 50 key supplier locations and set criteria for when alarms needed to be sounded (for example, when an earthquake occurs within 200 miles of a site).[116]

Cisco's supply chain incident management team "is the volunteer fire department for supply chain incidents," says Steele. "We have a core team of eight people, and we can grow up to 250 people around the world if needed, as was the case with the tsunami in Japan. We operate a war

[113] Ibid.,110.
[114] Ibid., 110, 112.
[115] Ibid., 112.
[116] Ibid., 112.

room when a crisis hits. We use playbooks and constant real-time monitoring. We can stand up a war room within a couple of hours of an event."[117]

Results

Cisco's SCRM program is an unqualified success, as evidenced during the 2011 Japanese earthquake and tsunami disaster.

> *"We had $2 billion worth of revenue potentially at risk in Japan at the time with regard to our manufacturing contractors," reports Steele. "Within 15 minutes of the earthquake, we got notification that it had occurred and that it was big. Within 1 hour, our whole team on phone watching it on CNN. Within 12 hours, we called our CEO and said we need all hands on deck.*
>
> *"A lot of companies went through this event, but many of them didn't take it seriously for a week, and then took three weeks to respond," Steele continues. "They weren't prepared and they got their heads taken off.*
>
> *"Our response, on the other hand, got underway within 12 hours. Using our supplier BCP database, we could graphically show on a map where our suppliers were located in northeast Japan. We could double click on those dots and see which products were being made at which locations, and what products were potentially going to be affected. We could quickly cut through the chaos, see who might be impacted, how to get hold of them, and what we needed to do to mitigate our risk.*
>
> *"Despite the fact that the Japanese disaster potentially could have affected 300 tier 1 suppliers, and about 7000 parts numbers, we experienced virtually no negative revenue impact."*[118]

Case #3: McAfee

Securing the Cyber Supply Chain

When most people think of McAfee Inc., they think of security and virus protection software. But many may not realize that McAfee's portfolio includes intrusion detection and prevention products that cost anywhere from 11 cents all the way up to the price of an E-class Mercedes.

Since its founding in 1987, Santa Clara, Calif.-based McAfee has grown into the world's largest dedicated security technology company. The statistics tell the story: Annual sales in excess of $2 billion; 125 million users, including 94 percent of Fortune 100 companies; more than 180 million mobile devices are shipped with McAfee; 120 countries make up McAfee's global footprint.

---

[117] Steele, James. "Cisco." Presented at the Annual Global Conference, Council of Supply Chain Management Professionals, Atlanta, GA, September 2012.
[118] Ibid.

In February 2011, the company was acquired by Intel Corporation for more than $7 billion. Wall Street analysts were somewhat mystified by the acquisition, but to Dennis Omanoff, who until December 2011 served as McAfee's senior vice president, chief supply chain officer, chief procurement officer, corporate facilities and real estate, it made perfect sense. With cyber security intrusions and threats rising exponentially for every aspect of technology—from silicon chips, smartphones, enterprise servers, and cloud computing to national defense and critical infrastructure grids—there's a pressing need to embed security at new levels, including in the chip itself.

This case study is based on multiple interviews with Dennis Omanoff, conducted while he was at McAfee. The interviews served the basis for an article published in the January 2012 issue of *Inbound Logistics* magazine, as well as to provide content for this report. Shortly after our interviews, Omanoff left McAfee to accept a position as senior vice president, supply chain and procurement for Seagate Technologies. [119]

Cyber Threats in the Supply Chain

"Before Sept. 11, 2001," Omanoff observes, "most supply chain professionals focused security measures on preventing the theft of valuable goods in their manufacturing and transportation operations. After Sept. 11, we focused on preventing weapons of mass destruction—or disruption—from being placed in cargo containers or other conveyances headed to the United States.

Today, there's a potentially more destructive—and often overlooked— danger to the supply chain community: cyber security threats. The volume and sophistication of cyber threats from totalitarian governments or nefarious individuals is increasing exponentially.

This 21st-century threat jeopardizes not only our information infrastructure, but the supply chain community, and at all levels of high-tech software and hardware products that connect with local or enterprise-wide networks, both hardwired and wireless.

Concerns about the "injection of viruses" into high-tech hardware products during their journey from manufacturing sources to customer delivery continue to grow. These concerns are especially high with regard to government agencies. More than natural disasters, financial instability, or political upheavals, what keeps me up at night is the fear that bad guys are injecting into products bad stuff that can disrupt, bring down, or steal confidential information from networks.

In the past two years, persistent and highly organized cyber-attacks such as Stuxnet, Aurora, Wikileaks, ShadyRAT and Night Dragon illustrate how cleverly the bad guys can worm their

[119] Excepted/adapted with permission from Harrington, Lisa H. "Security Guard: Questions and Answers with Dennis Omanoff." *Inbound Logistics.* January 2012. Available at http://www.inboundlogistics.com/cms/article/security-guard-questions-and-answers-with-dennis-omanoff/.

way into the world's most protected networks and either sabotage them, steal intellectual property, or compromise government trade or military secrets.

So the question is, how safe are our networked products—from software to computers to servers? How do we protect the integrity of our supply chains and the products they carry?

Protection through Obfuscation

In supply chains, including that of the DoD, we are always concerned about doing things better, faster, and cheaper. So we've outsourced to China. But that has created an unforeseen risk—one that is of grave concern to national security. Night Dragon and other cyber threats are examples of nation-states or totalitarian regimes aggressively seeking intellectual property and testing cyber terrorism and warfare.

China is neither safe nor secure as a production source. There are no data loss or IP protection mechanisms—a situation that could subject product to inadvertent dangers. When you see a picture of our stealth bomber sitting in China, or learn that its ballistic missiles are based on our design, you have to wonder how that happened.

In a meeting at DoD, an undersecretary of defense (supply chain) asked for McAfee's help. "First, I want you to obfuscate the supply chain so no one can figure out what is in a box being delivered to a defense agency," he said. "Second, I'd like a supply chain where the contingent labor is a group we can qualify. Third, I want my suppliers' CEOs to be willing to take a call from the Secretary of Defense in time of dire need. Finally, I want to establish a Trusted Source program."

McAfee has worked very hard to achieve these goals.

To obfuscate our supply chain, we architected a global operation based on late-stage postponement. Component parts are secured via distribution partners from multiple locations, then assembled, converted into finished products, and shipped by trusted sources. Any of our products can be made or assembled from any of our strategic locations in Europe, North America, or Asia, and shipped to any other locations, almost at a moment's notice.

The final assembly and hardware conversion—whether software, adaptor cards, or some type of interface card—and final shipment can be postponed until the last minute, and done very quickly. We aim for 20 minutes from the time an un-forecasted order comes in (lead time on predictable orders is 30 days). With this type of sense-and-respond network, we obfuscate the trail of quickly assembled final products so that it's nearly impossible to know beforehand what a product is and where it's headed—whether to an energy grid, nuclear power plant, or government agency. This helps protect our 'sensitive' customers.

Further, it's critical to keep inventory and backlog as low as possible. As the saying goes, "Inventory at rest is inventory at risk." Keeping inventory moving not only makes good financial sense, but also good security sense.

McAfee also required all suppliers to have an information security policy in place for data loss prevention and system control. Most of our suppliers agreed.

Making these changes in our supply chain was no small task. After all, we have 35,000 SKUs on our price book.

How did we do it? Take the example of a PC, which is comprised of a processor, a power supply, some physical packaging, a combination of flash memory, and some spinning media. We worked with our 16 product engineering teams to coalesce our products to use the fewest base items, then create 10 basic configurations, enabling us to make every product we offer out of 170 SKUs. Then we add the software load at the last minute.

By simplifying our product configuration to make late-stage postponement possible, we reap some big rewards. We turn inventory 55 times a year and our unshipped backlog is 0.2 percent. Usually, you can't achieve both high turns and low backlog at the same time.

Other Anti-infection Measures

At McAfee, a number of strict measures have been put into place to protect and prevent the "infection" of products, especially hardware-assisted security systems.

These include the following policies and practices.

- **Data loss policies.** All of McAfee's suppliers must have an information security policy in place for data loss prevention (DLP) and system control that provides complete protection of both network and host leakage. McAfee's Security Policy for Data Loss Prevention & Systems Control is reproduced below in the highlighted section.
- **Trusted source network.** In addition to strict qualifying standards for its suppliers, McAfee has architected a global supply chain operation where component parts are secured via distribution partners from multiple locations and then assembled, converted into finished products and shipped by trusted sources chosen by customer preference. Any of our products can be made or assembled from any of our strategic locations in Europe, North America or Asia and also shipped to any other locations, almost at a moment's notice.
- **Sense-and-respond fulfillment.** The final assembly and hardware conversion, whether it's software, adaptor cards or some type of interface card, and final shipment can be done very quickly – we aim for 20 minutes from the time an un-forecasted order comes in (aim for 30-day lead time on predictable orders). With this type of sense and respond network, we're able to obfuscate the trail of the quickly assembled final product so that

it's nearly impossible to know beforehand where it's headed, whether it's an energy grid, nuclear power plant or government agency.

- **Inventory velocity policy**. Further, it's critical to keep as low an inventory and backlog as possible – as the saying goes, "Inventory at rest is inventory at risk". This not only makes good security sense, but also good business sense.
- **Regionalized but trusted partners**. By having a geographically dispersed supply chain, and trusted partners that can operate as a single unit, we can satisfy the unique requirements of customers in various regions. For example, "Assembled in the USA" verification helps meet stringent U.S. (and some European) government requirements. But similar in-nation rules and incentives are imposed in other parts of the world, necessitating a highly flexible and segmented supply chain.

These different security requirements can be met with what Dr. Hau Lee at Stanford University calls "multi-polar, differentiated supply chains." In other words, complete regionalized supply chains working either independently or as a unified operation can meet localized and globalized customer demands while also creating an operation that protects products from being sabotaged by the latest cyber virus somewhere along the way.

Case #4: NASA

Protecting Against Counterfeit Components

Problem

Identification, removal, and prevention of counterfeit electronics in the National Aeronautics and Space Administration's (NASA) supply chain is critical to maintaining the safety of personnel and the integrity of components used in satellites, rockets, communications systems and computers. As is the case with DoD, counterfeit parts can threaten missions and, more importantly, lives. For this reason, NASA goes to exhausting lengths to ensure component quality and integrity. This case study discusses NASA's approach to ensuring component quality through a rigorous quality assurance process.

Anti-counterfeit Policy Approach

NASA was an early mover in adoption of anti-counterfeiting policies and industry standards. In September 2007, the SAE International G-19 Committee formed with representatives from U.S. Department of Homeland Security, U.S. Department of Defense, NASA, original component manufacturers, contract assembly manufacturers, distributors, and industry suppliers and associations. This committee worked to develop a counterfeit electronic parts control plan

known as SAE International AS5553 ("Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition"),[120] which it formally released in April 2009.

NASA was the first government agency to adopt SAE International AS5553 on November 3, 2008 before the official release of the plan (NASA Policy Directive NPD8730.2C – "NASA Parts Policy") DoD followed suit in August 2009. The plan standardizes methods for electronic counterfeit part mitigation. It outlines processes for electronic design/parts management, supplier management, procurement, part verification, materials control, and response strategies when suspect parts are found.[121][122]

To implement the new policy, NASA focused on educating and training its people and its suppliers. The agency provided awareness briefings, reported all ERAI counterfeit parts alerts to all NASA organizations, and hosted bi-annual quality leadership forums and annual supplier quality conferences. Training included (1) a review of the Independent Distributors of Electronics Association (IDEA) Inspection Standard 1010A to all NASA centers and prime contractors; (2) a course in Counterfeit Parts Avoidance for inspectors, operators, auditors, and suppliers; and (3) an AS5553 course and training module.[123]

One example of NASA's efforts to eradicate quality issues and preempt counterfeit risk is the Goddard Space Flight Center (GSFC) supplier assessment program. Figure 22 demonstrates the assessment process. GSFC selects each prime contract supplier for an assessment every two years. Lower tier supplier assessment considerations include high-risk or critical suppliers, common supplier for multiple mission projects, new suppliers, supplier issue or concern elevated to senior management, or a project office request. The assessment includes a review of procedures and processes, sampling of documents or records, interviews of management and personnel, and direct observation.

From this review, the assessment team generates a report that includes corrective and preventive actions. Then, the report is distributed to the supplier, NASA GSFC offices, and other NASA centers or agencies as requested.[124]

---

[120] Zulueta, Phil. "SAE International Releases Standard AS5553 - Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition." NASA Jet Propulsion Laboratory. Accessed October 18, 2012. Available at http://www.pacs.arizona.edu/files/S021306_Reference_Document_AS5553.pdf.

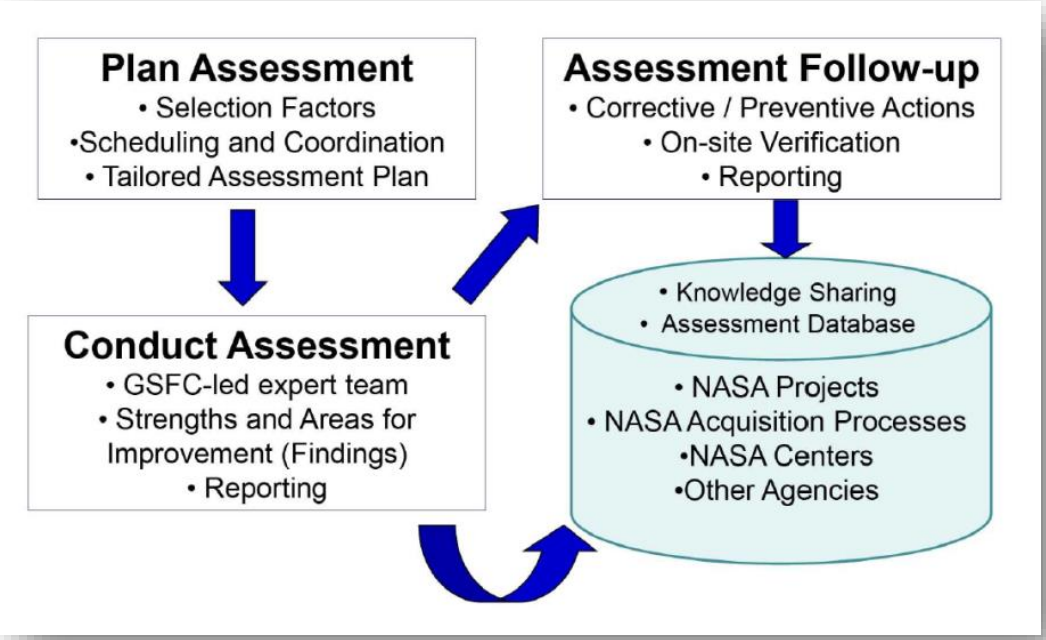
[121] Zulueta, Phil. "Counterfeit Electronics: NASA Update." NASA Jet Propulsion Laboratory and California Institute of Technology. Presented June 29, 2011. Accessed October 18, 2012. Available at http://nepp.nasa.gov/workshops/etw2012/submissions/talks/Wednesday/1130%20-%20Counterfeit%20Electronics%20-%20NASA%20Update.pdf.

[122] Aerospace AS5553 Resource Center. "What is AS5553?" 2009. Accessed October 18, 2012. Available at http://www.as5553.com/.

[123] "SAE AS5553: A New Standard in the Fight Against Counterfeit Electronic Parts." NASA Jet Propulsion Laboratory/California Institute of Technology. November 3, 2009. Accessed October 4, 2012. Available at http://www.dscc.dla.mil/downloads/psmc/Nov09/NewStdInFightAgainstCounterfeitElectronicParts.pdf.

[124] Root, Jonathon. "GSFC Supplier Assessments." Safety and Mission Assurance Directorate, Goddard Space Flight Center. October 18, 2011. Accessed October 22, 2012. Available at http://supplychain.gsfc.nasa.gov/sc2011j.rootasof1020.ppt.pdf.

Figure 22: GFSC Supplier Assessments Overview



Source: Kelly, Michael P. "NASA/Goddard Space Flight Center
Supply Chain Management Program." Presented February 10-11, 2011 at PM Challenge. Accessed November 1, 2012
http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20110007132_2011005476.pdf.

During execution of the corrective and preventive action plan, the NASA team performs a root cause analysis to determine causes and effects of issues; and a cost-benefit analysis of corrective actions. The team also determines timing and assesses short- and long-term containment actions. Finally, the team works with the facility to implement corrective and preventive actions based on priority, impact, and risk.[125] As a result of supplier assessments at GSFC, the team addressed issues such as obsolete procedures referenced, expired materials, logs not correct or not signed/dated, calibration supplier contract inadequate, and mishap reporting not accurate.[126]

Results

NASA's success in reducing counterfeit electronics by adopting SAE International AS5553 helped form a new multi-agency working group. In 2010, 14 U.S. Government agencies, including Intellectual Property Enforcement Coordinator (IPEC), Office of Management and Budget (OMB), Department of Defense (DOD), National Aeronautics and Space Administration (NASA), Department of Energy (DOE), and General Services Administration (GSA), formed the USG Inter-Agency Anti-Counterfeiting Working Group to identify areas of common interest and

[125] Brunello, Brenda and Charles Robinson. "GSFC Supplier Assessments: Mitigating Risks through Corrective Action." NASA Safety Center. Presented October 18, 2011. Accessed October 22, 2012. Available at http://supplychain.gsfc.nasa.gov/sc2011b.brunelloc.robinsonasof1017.pdf.
[126] Sivcovich, Ken. "NASA Supplier Assessment Experience." DRS Sensors & Targeting Systems. Presented October 20, 2010. Accessed October 22, 2012. Available at http://supplychain.gsfc.nasa.gov/SC2010-K.Sivcovich.pdf.

compare progress and best practices to ultimately eliminate counterfeits in their supply chains and develop a consistent and effective government-wide approach to reducing the U.S. government's vulnerability to counterfeit products.[127] Additionally, the National Aeronautics and Space Administration Authorization Act of 2010 (Senate bill S. 3729) emphasized the improvement of NASA's efforts against counterfeits.[128]

As a result of the changes implemented from the assessments, NASA adjusted its purchasing information requirements. Current requirements include (1) supply chain traceability to the OCM or aftermarket manufacturer that identifies the name and location of all of the supply chain intermediaries from the part manufacturer to the direct source of the product for the seller and (2) specify flow down of applicable requirements of this document to applicable contractors and their sub-contractors.[129]

In a continued effort to focus on its people and after the results from assessments, NASA started working on the education of its suppliers in May 2012 through sharing current policy and requirements with suppliers, sending out new electronic component surveys to assess risk level, and narrowing down the specifics of what qualifies as a "Trusted Supplier" to publish specific requirements available to all suppliers.[130]

Continually educating and assessing suppliers remains essential to securing NASA's supply chain as the number of suppliers continues to increase. The GSFC supplier assessment program applied to all NASA facilities and programs help NASA assure mission success.

[127] 2010 U.S. Intellectual Property Enforcement Coordinator Strategic Plan. Executive Office of the President of the United States. February 2011. Accessed October 18, 2012. Available at http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_report_feb2011.pdf.
[128] Zulueta, Phil. "Counterfeit Electronics: NASA Update." NASA Jet Propulsion Laboratory and California Institute of Technology. Presented June 29, 2011. Accessed October 18, 2012. Available at http://nepp.nasa.gov/workshops/etw2012/submissions/talks/Wednesday/1130%20-%20Counterfeit%20Electronics%20-%20NASA%20Update.pdf.
[129] Zulueta, Phil. "Industry Game Changers: SAE G-19 Standards Updates." Presented May 17, 2012 at ERAI Executive Conference. Accessed October 4, 2012. Available at http://www.erai.com/presentations/General%20Session%201/Industry%20Game%20Changes%20-%20Phil%20Zulueta.pdf.
[130] Foster, Steve. "Dryden Flight Research Center." NASA. Presented at Dryden Flight Research Center, 2012. Accessed October 4, 2012. Available at http://www.erai.com/presentations/General%20Session%201/NASA-Steve%20Foster.pdf.

VI. Solutions, Implementation Challenges and Lessons Learned

Supply chain security is a moving target and as such, the work of ensuring it is never complete. This is true for any supply chain, whether public or private sector.

In this section of the report, we offer insights into the methodologies for and benefits of standardizing supply chain security efforts at DoD to produce better results; provide recommendations that DoD could consider incorporating into its existing efforts; outline security frameworks that deliver proven results; discuss implementation issues and challenges; and highlight lessons learned from across the global supply chain community.

SCSM cannot completely eliminate most threats. Instead, the goal is to minimize the impact of any type of threat within the supply chain – to make DoD's supply chain more resilient. Individual security measures typically deter/prevent, detect, delay, and/or respond/recover. All must be present and effectively executed in order to assure supply chain security.[131]

Standardizing Risk Assessment and Identification

The first step in managing supply chain security is to adopt consistent risk assessment/identification tools. DoD is working in this direction, but it nevertheless bears discussing here so as to provide the foundation for ongoing and future security improvement efforts. DoD and other federal agencies use a common risk equation, described below, to evaluate security risk and exposure.

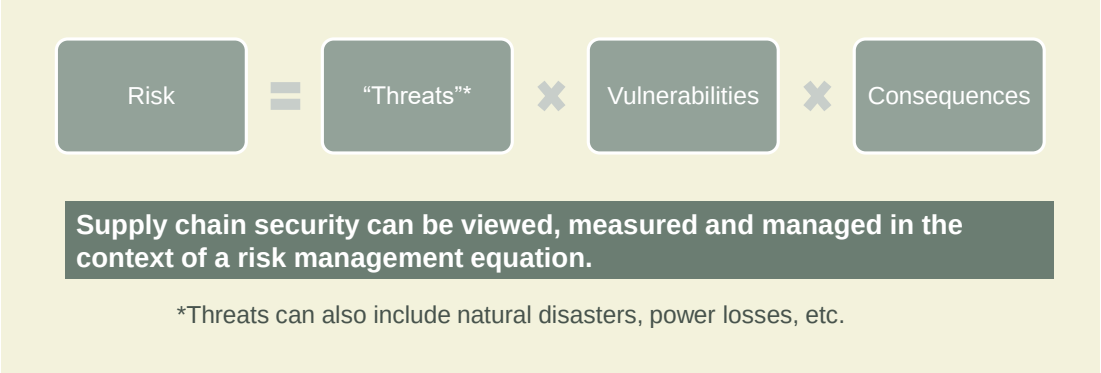
Determining risk is a qualitative/quantitative process of combining three evaluated components (Figure 23):[132]

- Threats (likelihood of occurrence)
- Vulnerabilities (weaknesses or gaps in security from established standards; a measure of security effectiveness)
- Consequences (impact of adverse occurrences)

[131] Pinkerton Consulting and Investigations, "Supply chain Security in 21st Century." Accessed September 13, 2012. Presentation available at http://www.securitas.com/Global/Pinkerton/Supply%20Chain%20Security.pdf

[132] Pinkerton Consulting and Investigations. "Risk Assessments and Risk Based Supply Chain Security." Accessed September 17, 2012. Presentation available at http://www.cosco-usa.com/omd/security/ctpat2010/2010-Seminar-Risk-Assessment-Training.pdf.

Figure 23: Supply Chain Risk Equation



Source: Center for Public Policy and Private Enterprise 2012

Threat Assessment:

The threat assessment takes a holistic look at all threats to the global supply chain, including:

Terrorism
Illegal weapons
Fire/explosion
Political unrest
Organized crime
Illegal currency
Contraband
Human smuggling, stowaways
Economic conditions
Labor problems
Product tampering
Counterfeits
Disease
Natural disasters
Industrial espionage
Theft

Vulnerability Assessment:

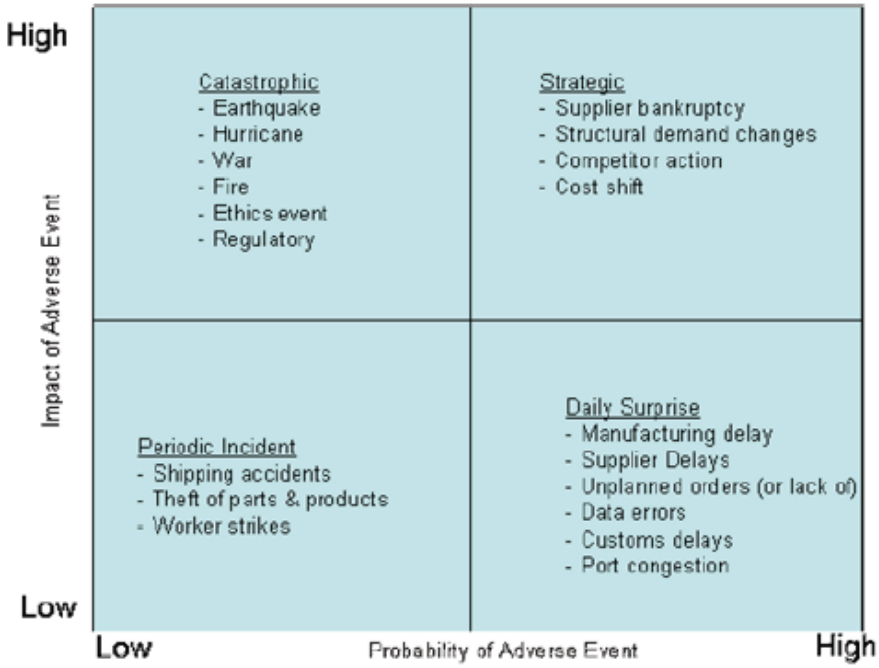
The vulnerability assessment identifies existing gaps and exploitable weaknesses (vulnerabilities) in established security standards at all points in the flow of material within the supply chain. These gaps fall into the following basic categories:

Business partner requirements
Personnel security
Physical security
Security training and threat awareness
Access controls
Procedural security
Information technology security
Securing the instruments of traffic or conveyances (e.g. container/trailer security)

Consequences Assessment

A consequences assessment identifies potential consequences of supply chain security issues and assigns a weighted value to the estimated impact on the organization. Figure 24 provides a grid approach to identifying impact and probability ranks to security events. This assessment helps support evaluation of potential consequences and responses. Supplier bankruptcy, for example, scores high in both probability of occurring and impact on the supply chain.

Figure 24: Impact and Probability Grid



Source: E2open. "Going Global is Risky Business: Gain Better Control to Maintain Profitability." Foster City, California, November 2, 2009. Available at http://hosteddocs.ittoolbox.com/riskybizwp.pdf.

Using the T x V x C framework, we can use a three-tiered matrix to assess supply chain security risk and quantify its impact in a DoD context. This matrix provides a consistent and easily understood assessment tool.

The first step is to analyze DoD supply chain security from a strategic, operational and tactical perspective. Figure 25 illustrates how a combination could be applied to identify DoD physical supply chain security issues and assign level-of-impact value to each issue (high, moderate, etc.). By assigning level of impact, DoD can prioritize its supply chain security investments and interventions.[133]

[133] Ibid.

Figure 25: Physical Supply Chain Level of Impact Analysis

	Physical Supply Chain	Rating
Strategic Tier	**Threats**: Terrorism, nation-state "attack", cyber warfare **Vulnerabilitie**s: Critical infrastructure **Consequences**: Shut down of single or multiple critical infrastructure sectors	High Moderate Low None
Operational Tier	**Threats**: Terrorism, nation-state "attack", cyber warfare, natural disasters **Vulnerabilities**: Supply chain operating capability, continuity, performance **Consequences**: Widespread supply chain security breach with major supply chain disruption. Inability to accomplish theater mission.	High Moderate Low None
Tactical Tier	**Threats**: Terrorist, criminal or activist activity, natural disasters **Vulnerabilities**: Cargo/facility/personnel security **Consequences**: Cost of goods lost, support interruption, damage/injury	High Moderate Low None

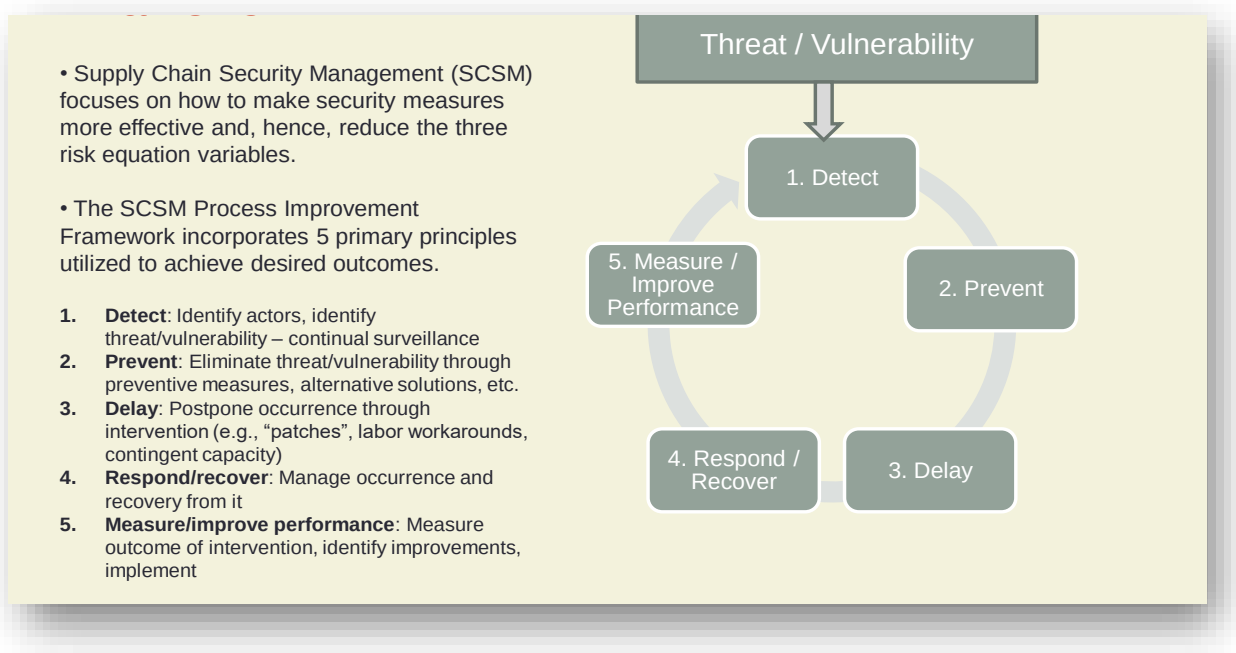
Source: Center for Public Policy and Private Enterprise 2012

Once the organization determines level of impact values for its supply chain security threats and vulnerabilities, the next step is to manage and/or reduce the impacts and risks?

- Lower the threats? How?
- Lower the Vulnerabilities? How?
- Lower the consequences? How?

The next step in a comprehensive supply chain security management (SCSM) process is to focus on how to make security measures more effective and, hence, reduce the three risk equation variables (T x V x C). The SCSM Process Improvement Framework (Figure 26) incorporates five primary principles utilized to achieve desired outcomes, including detect, prevent, delay, respond/recover, and measure/improve performance. Figure 32 briefly describes/defines each of the five components in the process improvement framework. It should be noted that this process is continuous, constituting a framework for constant learning and improvement.

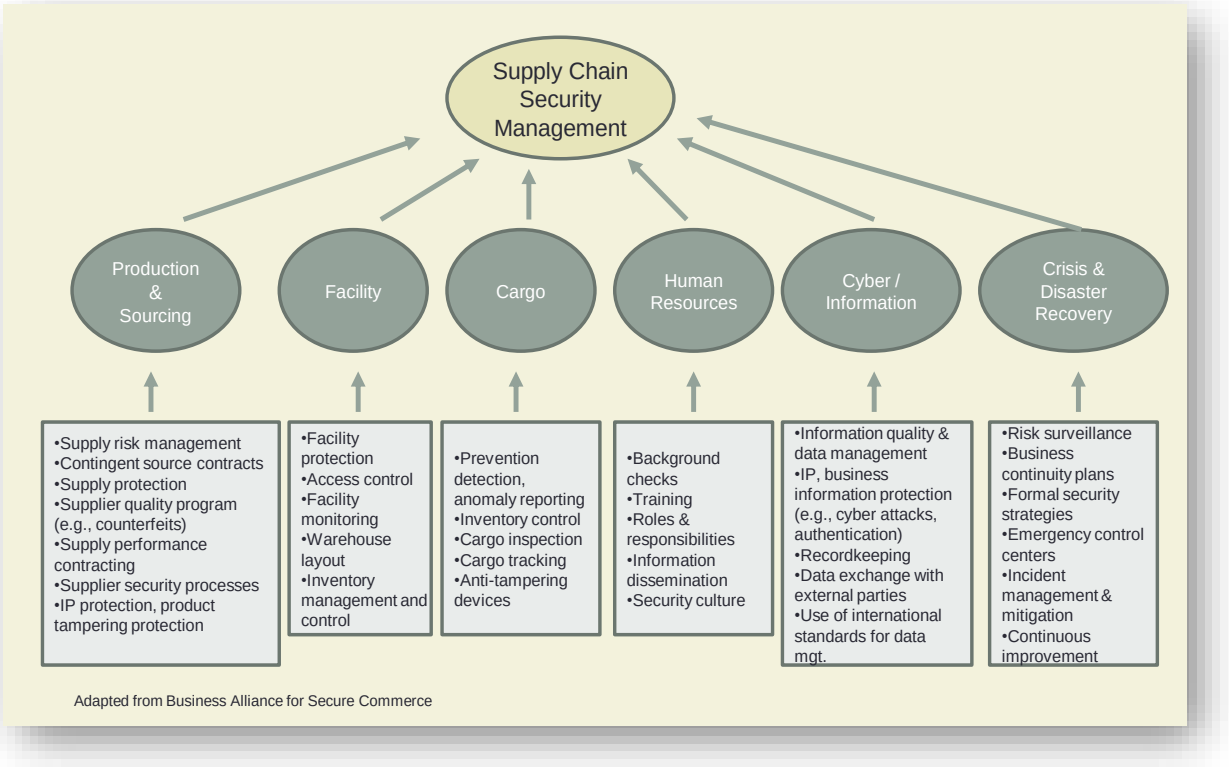
Figure 26: Supply Chain Security Process Improvement Framework



Source: Center for Public Policy and Private Enterprise 2012

The schematic in Figure 27 illustrates operational attributes that could make up a SCSM program. The "execution" activities – in the rectangles – support the core attributes (e.g., production/ sourcing, cargo, etc.) of a supply chain.

Figure 27: SCSM Operationalized



Source: Center for Public Policy and Private Enterprise 2012

Figure 28 suggests some sample supply chain security elements as applied to the physical supply chain, and broken down into categories – e.g., production and sourcing, facility, cargo.

Figure 28: Sample Supply Chain Security Program Elements

Category	Physical Supply Chain – Program Elements
Physical security	• Physical deterrents • Process/procedures • Documentation • Continual monitoring, sensors
Access control	• Secure identification • Access hierarchies and controls • Intrusion prevention
Personnel security	• Screening • Background checks • Procedural
Education & training	• Ongoing security training – all levels
Procedural security	• Documentation & manuals • Standardized function-specific procedures
IT security	• Secure access control • Accountability
Business partner security	• Documented security guidelines • Contractual requirements
Transportation security	• Inspection procedures • Cargo securement • Chain of custody protection • Documentation

Source: Center for Public Policy and Private Enterprise 2012

Develop a Process Catalog

To support the supply chain security program and framework, best practice organizations develop a process catalog which defines those processes critical to managing security effectively. These processes may be defined separately, but they are unlikely to operate in isolation from one another. In some cases, there will be interdependencies among these processes. At minimum, the process catalog should include clear documentation of:[134]

- A catalog that shows who does what (for example, using a cross-functional flowchart), what resources are required (for example, a configuration management database) and what actions/capabilities will be delivered

[134] McMillan, Rob. "The Security Processes You Must Get Right." Research Paper. Feb 24, 2011, 4.

- A matrix that establishes who is accountable for what decisions, and what other stakeholders are involved (for example, a responsible, accountable, consulted and informed [RACI] chart)
- Reporting metrics encapsulated in formal reports (for example, a balanced scorecard)
- Standing agenda items for steering committees and other relevant governance groups (for example, a review of balanced scorecard results[135]

Incident Response

The extent of the damage from a supply chain security incident largely depends on the quality of the response, says Rob McMillan of Gartner. It is therefore critical for the security organization to have a well-documented incident response process that has been successfully (and, if possible, repeatedly) exercised prior to an actual incident. There should also be defined and documented criteria for escalating the incident to crisis status, if the event presents a credible threat to the enterprise.[136]

The major steps in managing an incident are detection, assessment, response and learning:

- Detection may occur via any number of means, such as unusual activity detected by a security operations center monitoring a security information and event management platform, or an unauthorized change to a device detected by a secure configuration scanning activity.[137]
- Assessment and response may involve a number of disciplines outside the security and technical realms, such as line-of-business managers and risk, legal, media, and contract management specialists.[138]
- The learning phase is often neglected, but this is a serious mistake.

Metrics that should be reported include the occurrence of actual security events (for example, an actual penetration, as opposed to the number of scans against an external firewall), completion of Post incident reviews and progress tracking of remedial actions.[139]

Nine Security Practices

This following section provides nine practices that an organization should consider when creating the list of measures to employ as part of a cyber-security strategy. The practices build on and mesh with the basic T x V x C formula. Each practice is a blend of programmatic activities, validation/verification activities and requirements, as well as general and technical

[135] Ibid.
[136] McMillan, Rob/ The Security Processes You Must Get Right, Gartner Inc. Feb. 24, 2011.
[137] McMillan, Rob. "The Security Processes You Must Get Right." Gartner Inc. Feb 24, 2011.
[138] Ibid.
[139] Ibid.

implementation requirements. The programmatic and validation/verification activities are implemented by the acquiring organization.[140]

While these practices are written to apply to software supply chain security, many can easily be adapted to cover aspects of physical supply chain security. These practices are offered by the Department of Commerce's National Institute of Standards and Technology (NIST).

The nine practices include the following:[141]

1. Uniquely identify supply chain elements, processes, and actors
2. Assess the current state of supply chain security practice to establish the "as is" baseline and establish the "to be" baseline of supply chain security practice
3. Limit access and exposure within the supply chain
4. Create and maintain the provenance of elements, processes, tools, and data
5. Share information within strict limits
6. Perform SCRM awareness and training
7. Strengthen delivery mechanisms
8. Assure sustainment activities and processes
9. Manage disposal and final disposition activities throughout the system or element life cycle.

1. Uniquely identify supply chain elements, processes, and actors[142]

Knowing who and what is in an enterprise's supply chain is critical to gain visibility into what is happening within it, as well as monitoring and identifying suspicious or adverse events and activities. Without knowing who and what are in the supply chain, it is impossible to determine what happened, mitigate the incident, and prevent it from happening again. Uniquely identifying organizations, personnel, mission and element processes, communications/delivery paths and elements, and components and tools used on them establishes a foundational identity structure for assessment of ICT supply chain activities. Everything and everyone that participates in the supply chain should also be uniquely identifiable so that activities can be traced and responsible actors and entities defined (traceability).

2. Assess the current state of supply chain security practice to establish the "as is" baseline and establish the "to be" baseline of supply chain security practice[143]

To evaluate the "as is" state of supply chain security, organizations can use a *priority code* designation associated with each security control in the baselines. This coding system assists in making sequencing decisions for control implementation (i.e., a Priority Code 1 [P1] control has a higher priority for implementation than a Priority Code 2 [P2] control; a Priority Code 2 (P2)

---

[140] Bartol, Nadya, Jon Boyens, Rama Moorthy, Celia Paulsen, and Stephanie Shankles. "Notional Supply Chain Risk Management Practices for Federal Information Systems." U.S. Department of Commerce: National Institute of Standards and Technology. Draft NISTIR 7622, March 2012, 23-24. Available at http://csrc.nist.gov/publications/drafts/nistir-7622/second-public-draft_nistir-7622.pdf.
[141] Ibid.
[142] Ibid., 25-26.
[143] "Information Technology: Recommended Security Controls for Federal Information Systems and Organizations." National Institutes of Standards Technology. August 2009., D-1.

control has a higher priority for implementation than a Priority Code 3 [P3] control). This recommended sequencing prioritization helps ensure that foundational security controls upon which other controls depend are implemented first, thus enabling organizations to deploy controls in a more structured and timely manner in accordance with available resources.

3. Limit access and exposure within the supply chain[144]

Material that moves through the supply chain is subject to access by a variety of actors. It is critical to limit such access to only as much as necessary for those actors to perform their role(s) and to monitor that access for supply chain impact. Access control privileges can be defined with appropriate granularity in such a manner that only appropriate actors are permitted to monitor or change supply chain elements, element processes, organizations, organizational processes, information, communications, and systems covering the comprehensive supply chain.

4. Create and maintain provenance of elements, processes, tools and data[145]

All system elements originate somewhere and may be changed throughout their existence. The record of element origin and the changes tied to who made those changes is called provenance. Acquirers, integrators, and suppliers should maintain provenance of elements under their control to understand where the elements have been and who might have had an opportunity to change them.

Provenance is used when ascertaining the source of goods such as computer hardware to assess if they are genuine or counterfeit. Provenance allows for all changes from the baselines of components, component processes, information, systems, organizations, and organizational processes, to be reported to specific actors, functions, locales, or activities. Creating and maintaining provenance within the supply chain helps achieve greater traceability and is critical for understanding and mitigating risks. Doing so requires a process by which all changes to objects and activities within a supply chain and the persons, organizations, or processes responsible for authorizing and performing such changes are inventoried, monitored, recorded, and reported.

A number of industries are instituting or already have instituted provenance-type systems and procedures to assure product integrity. Provenance systems will become more widespread.

5. Share information within strict limits[146]

Supply chain actors need to share data and information. The data and information that may be shared spans the entire system or element life cycle and the entire supply chain. Content to be shared may include data and information about the use of elements, users, acquirer, integrator, or

[144] Bartol, Nadya, Jon Boyens, Rama Moorthy, Celia Paulsen, and Stephanie Shankles. "Notional Supply Chain Risk Management Practices for Federal Information Systems." U.S. Department of Commerce: National Institute of Standards and Technology. Draft NISTIR 7622, March 2012, 29. Available at http://csrc.nist.gov/publications/drafts/nistir-7622/second-public-draft_nistir-7622.pdf.
[145] Ibid., 33.
[146] Ibid., 37.

supplier organizations, as well as information regarding issues that have been identified or raised regarding specific elements.

Access to information, however, should be strictly controlled using a permission-based system. This system gives access to individuals only at the level appropriate to their role in the supply chain – and no more than that. The information access control system also should include a mechanism with which to track who accessed the information, when, where and for what purpose.

Similar access control should be instituted and maintained for the physical supply chain as well.

6. Perform supply chain risk management awareness and training[147]

A strong supply chain risk mitigation strategy will not succeed unless significant attention is given to training personnel on supply chain policy, procedures, and applicable management, operational, and technical controls and practices. NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, for example, provides guidelines for establishing and maintaining a comprehensive awareness and training program with regard to the information supply chain.

Additionally, the ISO/IEC 27001 information security management standard and the ISO 28000:2007 supply chain process integration and certification standard provide an organization-wide program that includes training. These ISO standards can be used as foundational frameworks for training personnel in supply chain security risk management.

7. Strengthen delivery mechanisms[148]

Delivery can be both physical (e.g., of equipment/goods) and virtual (e.g., software modules and patches). Delivery, as a basic output of any supply chain, occurs at any point across a system life cycle, among multiple parties and multiple links of a given supply chain.

Because delivery may be compromised anywhere along the supply chain and system or element life cycle, both physical and virtual element delivery mechanisms should adequately protect the confidentiality, integrity, or availability of systems and elements delivered through the supply chain. Therefore, it is critical to develop security processes that protect and ensure the integrity of all delivery activities. The goal of this strengthening is to reduce and/or eliminate opportunities for unauthorized access or exposure to the element, processes and system, as well as information about their uses, which can result in unauthorized modification (including substitution and subversion) or redirection by active adversaries to an alternate location.

[147] Ibid., 44-45.
[148] Ibid., 61.

8. Assure sustainment activities and processes[149]

The sustainment process begins when an element or a system goes operational, and ends when it enters the disposal process. This includes maintenance, upgrade, patching, element replacement (e.g., spare part, alternate supply) and other activities that keep the system or element operational.

Any change to the elements, system, or process can introduce opportunities for subversion throughout the supply chain. These changes can occur during any stage of the system or element life cycle. The sustainment processes, therefore, should limit opportunities and means for compromise of confidentiality, availability, and integrity of elements and operational processes. All actors in a supply chain should understand, be equipped to support, and be held accountable for security throughout the entire sustainment cycle. This practice applies to both the bounded operational systems within the acquirers' environment, as well as the outsourced operational systems or activities provided by a third party.

9. Manage disposal and final disposition activities throughout the system or element life cycle[150]

Disposal of systems, material, components, data or other defense-related items must be managed throughout the entire lifecycle of that item in order to protect against security breaches. The disposition process should not be taken casually, and should be viewed as a critical component of any lifecycle management plan. Secure disposal and disposition addresses both the disposal of elements and tools as well as the documentation that support those items. Poor disposal procedures can lead to unauthorized access to systems and components.

Unfortunately, acquirers often neglect to define rules for disposal, thereby increasing the chances of compromise. NIST SP 800-88, *Guidelines for Media Sanitization*, for example, assists organizations in implementing a media sanitization program with proper and applicable techniques and controls for sanitization and disposal decisions.

Best Practice Protection against Counterfeits

Switching to the topic of securing against counterfeits in the DoD supply chain, best practice organizations adopt policies and practices that are geared toward product traceability and pedigree management. These practices emphasize before-the-fact prevention rather than after-the-fact detection and inspection. They are based on the premise that it is much easier to prevent counterfeits from entering the DoD supply stream in the first place than it is to search for them post-acquisition.

The policy and practices listed below were written to cover electronic component counterfeits, but are applicable with some adaptation to other products. Policy and practices should include the following:[151]

[149] Ibid., 65.
[150] Ibid., 70.

- Specify a preference (where possible) for procurement of electronic components from Original Component Manufacturer (OCMs), their authorized / franchised distributors, or through suppliers that furnish electronic components acquired from OCMs or their authorized distributors
- Specify extra measures to be undertaken and/or employed when procuring from independent distributors and brokers
- Provide universal definitions for "counterfeit" as relates to electronic components as well as for "franchised or authorized distributor", "independent distributor" and "broker"
- Review FAR Part 6 to determine the extent, if any, to which procurement activities are constrained from excluding bidders that are not the OCM or its authorized or franchised distributors from offering components
- Issue written guidance to clarify the FAR Part 6 exception by (1) defining OCMs or their authorized or franchised distributors as "responsible sources" and (2) requiring components be obtained from a limited number of responsible sources.

Policies and practices also should include the following:[152]

- Establish GIDEP as the repository for receiving and disseminating counterfeit case reports
- Provide qualified, limited immunity from third party suits to contractors, OCMs, and component suppliers that report in good faith suspect counterfeit components via GIDEP, and cooperate with each other in assessing whether or not a given item is counterfeit
- Establish contractual requirements and presumptions to increase sharing of counterfeit electronic component findings in order to alert other potential users in the defense and aerospace industries, government agencies, and law enforcement.

Implementation Challenges

Improving supply chain security at DoD poses many challenges. Some of these are unique to DoD due to the nature of the agency's mission; others are common across public and private sector supply chains alike. Key challenges fall into several categories:

- Organizational change
- Security strategy and focus
- Supplier relationship issues
- Information systems issues

Organizational change

Challenge: *DoD faces organizational issues in evolving its approach to supply chain security to a more risk-based, resiliency model.*

---

[151] Livingston, Henry. "Securing the DOD Supply Chain from the Risks of Counterfeit Electronic Components: Recommendations on Policies and Implementation Strategy." *BAE Systems Electronic Solutions*. October 18, 2010, 2.
[152] Ibid.

Entrenched organizational culture, structure, processes and skill sets must be changed in order for supply chain security to be addressed on a more holistic, end-to-end basis. In nearly all situations, organizational issues represent the biggest hurdles to effective supply chain security. DoD is no exception to this rule. Silo-ed organizational structure opens the door to supply chain security breaches, vulnerabilities and risk.

Those organizations that have the greatest success securing their supply chains – and the products they carry - deploy cross-functional teams to lead the effort. In the corporate world, these cross-functional teams consist of a combination of leaders from finance, legal, risk, and operations (e.g., procurement, logistics and manufacturing). Human resources representatives may be included on this team. Others include their insurance company or broker in their team discussions.[153]

These teams continuously assess, quantify, categorize, prioritize and manage risks centrally. They have access to 24/7 monitoring and alerting capability which provides an early warning system. Early detection arms the right people with the information they need to act on the situation or event. Pre-determined collaboration and action plans – playbooks – are put in motion. This collaborative, cross-functional approach equips the organization to deal more effectively with the security issue – whatever it may be - and shortens time to recover.

The support of senior leadership in moving toward this cross-functional security management model is critical. As a recent report from the World Economic Forum on transport and supply chain security points out, "The strategic and operational decisions required to build resiliency are often beyond the direct control of any one player and need to be the focus of collaborative activity. This requires the support of senior leadership in the organizations concerned."[154]

DoD has begun the process of developing supply chain risk plans for its programs – identifying what risks exist. Figuring out what to do about those risks – i.e., developing the kinds of "playbooks" that Cisco deploys when a disaster strikes its supply chain – is a far more complex task.

Security Strategy and Focus

Challenge. *Migrating to an end-to-end supply chain strategy that focuses on protecting missions as opposed to securing assets will require a major shift in operational strategy and tactics.*

As Accenture notes, most organizations focus their supply chain security strategies on protecting and securing assets, rather than on ensuring mission resiliency. As part of this asset-based focus, there is a tendency to focus on pieces and parts of the supply chain, rather than on the supply chain as an interconnected whole. The result is an incomplete picture of security and a sub-optimally integrated strategy for reducing risk and ensuring the integrity of the supply chain as a

[153] Ibid, 11.
[154] World Economic Forum. "New Models for Addressing Supply Chain and Transport Risk." Geneva, Switzerland, 2012, 11. Accessed August 1, 2012. Presentation available at http://www.weforum.org/reports/new-models-addressing-supply-chain-and-transport-risk.

whole, and of the materiel that flows through the supply chain. This description fits the DoD supply chain.

As DoD continues to migrate to a risk-based approach to managing supply chain security, and develop PPPs, it faces the challenge of creating a sentinel mechanism for continually scanning the supply chain for threats and vulnerabilities. Creating this sentinel mechanism puts the PPP updating process on a more real-time basis vs. simply publishing periodic static updates on supply chain security risks. Effectively, the idea would be to create a supply chain security control tower, with management dashboard, real-time alerts, analytics and other toolsets aimed at optimizing supply chain security.

This control tower and supporting toolsets would also be useful in evaluating new or different supply chain operating models.

Information Systems

Challenge. *Address information gaps and the ongoing need for robust information systems to monitor supply chain security and provide visibility into product flows, threat alerting, performance tracking, analytics and process management to support effective decision-making.* Building an information architecture to address the challenge of supply chain security monitoring and alerting is no small task. It is possible, however, as the Cisco case study illustrates.

Part of building this information gathering mechanism involves identifying and gaining consensus on what "signals" are the most appropriate to monitor under enhanced, ongoing scrutiny – as in the pharmaceutical industry model which tracks such things as change in the price of a key raw material; establishing the mechanisms for scanning for these signals; and then determining the relevance of the results based on pre-determined risk management strategy.

Supplier Management

Challenge: *Orchestrate greater collaboration and cooperation on all areas of supply chain security between DoD and its expansive supplier base.*

Supply chains by nature are boundary spanning entities which, in DoD's case, incorporate thousands of actors/participants all over the globe. DoD's traditional supplier relationships are transactional in nature, and as such, operate at arms' length. Collaboration on such critical issues as supply chain security in this context is difficult if not impossible.

To truly improve supply chain security requires a change in DoD-supplier relationships toward a collaborative model in which all parties work together to achieve the desired outcome of protecting the supply chain and the products within it. Achieving a more collaborative relationship requires:

- Effective program protection policies which are thoroughly developed, shared, understood and executed
- Education and training for internal and external partners and constituencies

- A shared risk assessment framework with scorecarding and risk prioritization.

Recommendations

We have described a number of best practices for supply chain security management that are in place in the public and private sectors. In some form or another, these measures could be adapted to DoD. A listing of these recommendations would include:

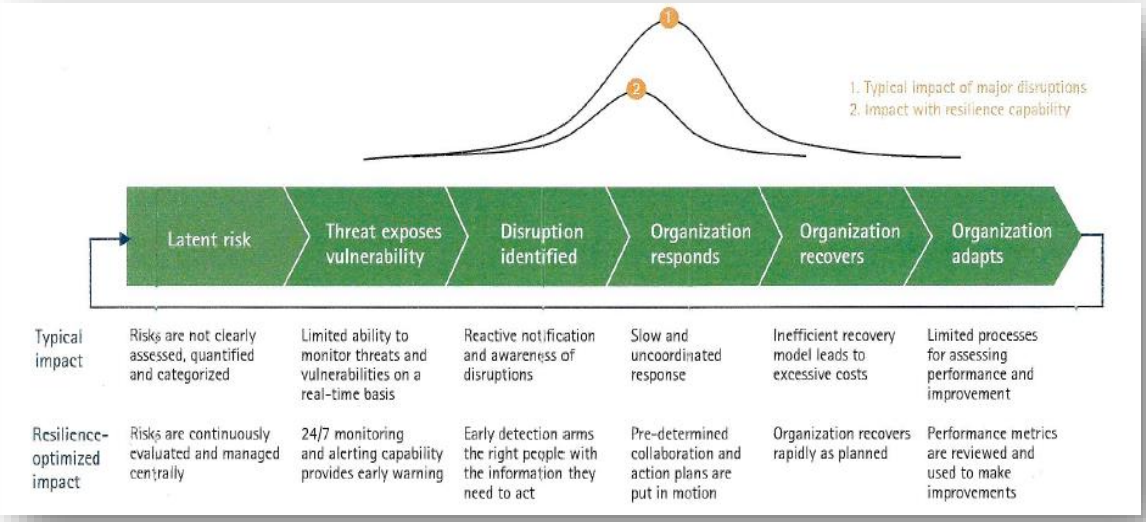
- Continue rolling out SCRM efforts underway
- Prioritize resources based on criticality and risk impact; develop a risk register
- Focus on mission resilience vs. asset protection; map time-to-recover
- Partner with industry; institutionalize security collaboration; develop the trusted network system
- Establish signal detection monitoring and alerting capabilities
- Implement change incrementally based on prioritization
- Institute metrics and continuous improvement mechanisms and frameworks
- Invest in visibility systems – e.g., dashboards, control tower monitoring technologies
- Include supply chain/program de-risking as part of platform initial design
- Adopt regionalized supply chains to reduce supplier and transport risk

Benefits of a More Secure Supply Chain at DoD

Improving supply chain security generates measurable and ongoing benefits for any organization, including DoD. These benefits translate into cost savings, better visibility, improved service, protected product integrity, and overall improved support for the warfighter.

Adopting a holistic view of supply chain risk, and addressing it from the perspective of managing and improving resilience produces better results than simply protecting assets, studies show. Figure 29 compares and contrasts how a focus on building resilience capability across the supply chain benefits the chain as a whole.

Figure 29: Holistic Lifecycle-focused Resilience Capability as Risk-reduction Tool



Source: Accenture. "Keeping Ahead of Supply Chain Risk and Uncertainty." 2008, 4. Available at http://www.oracle.com/us/products/applications/accenture-oracle-risk-pov-bwp-069959.pdf.

On a more specific level, improving supply chain security at DoD could produce benefits in the following areas:[155]

- Improved inventory management across the supply chain - reduction in incorrect quantity received; reduced inventory levels; improved inventory tracking and management; reduced theft, diversion, adulteration and counterfeits.
- Improved product safety - better security practices from acquisition to disposal protects product/system integrity; reduces theft/loss/pilferage; reduces tampering, damage, fraud; reduced damage, fraud and counterfeits.
- Improved service - service level to "customers" improves in several ways, including improved on-time deliveries, increased item fill-rate and a reduction in each of the following areas:
    - the number of back-orders
    - the frequency of cancelled orders and
    - defective products delivered.
- Cost savings - cost savings associated with improved inventory management; reduction in waste, counterfeits, shrinkage, loss and damage. Improved control of product flows accelerates supply chain throughout.

[155] Pelleg-Gillai, Barchi, Gauri Bhat, and Lesley Sept. "*Innovators in Supply Chain Security: Better Security Drives Business Value." Stanford University: The Manufacturing Institute,* July 2006, 15-23.

- Improved visibility - better visibility to the location and condition of goods as they move along the supply chain. In particular, visibility improvement benefits resulted from:
    - Access to data – improved accessibility to supply chain data, including internal and external data.
    - Timelines of data - improvement in the timeliness of supply chain information.
    - Data accuracy - reduced inaccuracies in supply chain data.
    - Cost savings attributed to improved supply chain visibility – e.g., knowing where products are in the supply chain.
    - Better "early warning" systems through real-or near real – time event monitoring.
- Greater resilience - reduced the problem identification time, reduced response time; shortened problem resolution time.

In the private sector, companies find clear and substantial return on investment for supply chain security improvements. A study of manufacturing companies investing in supply chain security and resilience found numerous operational benefits, including a 38 percent reduction in lost cargo, 37 percent reduction in product tampering, 14 percent reduction in excess inventory, 47 percent improvement in on-time delivery, 26 percent reduction in customer attrition and 20 percent increase in new customers.[156]

[156] Accenture. "Keeping Ahead of Supply Chain Risk and Uncertainty." 2008, 6. Available at http://www.oracle.com/us/products/applications/accenture-oracle-risk-pov-bwp-069959.pdf.

VII. Conclusion

Reducing supply chain security risk whether for the physical or the information supply chain requires addressing all of the following areas, activities, product, processes and personnel within the acquisition life cycle:[157]

- Acquirer capabilities: policies and practices for defining the required security properties of a particular product or system
- Supplier capability: ensuring that a supplier has good security development and management practices in place throughout the life cycle
- Product security: assessing a completed product's potential for security compromises and determining critical risk mitigation requirements
- Product logistics: the methods for delivering the product to its user and determining how these methods guard against the introduction of malware while in transit
- Operational product control: ensuring that configuration and monitoring controls remain active as the product and its use evolve over time
- Disposal: ensuring software data and modules are effectively purged from hardware, locations.

Figure 30: Risk Management Innovation Road Map

	Trailer	Innovator
Policies	Risk managers are rarely involved in non-insurable discussions involving the supply chain	Risk managers are responsible for helping assess and manage both insurable and uninsurable supply chain risks
Processes	Supply chain risk management activities are ad hoc and inconsistent across groups and regions	Supply chain risk management processes are consistent and company-wide, with risk management activities and responsibilities embedded into existing supply chain processes and functions
People	Risk managers feel they lack sufficient organizational clout to sufficiently address supply chain risks	Formal cross-functional risk management team, which meets monthly or quarterly
Technology	No centralized way to assess and monitor supply chain risks across the enterprise, making it difficult to anticipate and quantify risks and impacts	Able to summarize total supply chain risk levels by country, supplier, or product; visibility to supply chain activities and disruptions
Performance Management	Supply chain managers are not motivated to focus on risk management	Supply chain managers have risk plans or metrics in their job descriptions and business goals

Source: Enslow, Beth, "Stemming the Rising Tide of Supply Chain Risks: How Risk Managers' Roles and Are Changing Responsibilities." Report by MARSH, April 15, 2008. Available at http://usa.marsh.com/Portals/9/Documents/Stemming-the-Tide_final_4-16-08.pdf.

Addressing the risks inherent in every phase of the DoD acquisition lifecycle is a shared responsibility of the program office, each supplier, and operations management. Both the security of the supply chain and the security of the resulting product or system need to be considered.

[157] Ellison, Robert J., John B. Goodenough, Charles B. Weinstock, and Carol Woody, "Evaluating and Mitigating Software Supply Chain Security Risks." Carnegie Mellon: Research, Technology, and System Solutions (RTSS) and CERT Programs. May 2010, 4-5. Available at http://www.sei.cmu.edu/reports/10tn016.pdf.

As Figure 30 notes, the roadmap to innovation in supply chain risk management is a five-pronged effort that includes changes in policies, processes, people, technology and performance management. Innovators adopt a more inclusive and holistic approach to managing supply chain security, and reap benefits across the entire organization as a result. We believe similar opportunities and benefits are available to DoD by pursuing ongoing security efforts and adopting new methodologies taken from best practice organizations.

Acknowledgements

This research was partially sponsored by Lockheed Martin, and we are especially grateful for the support provided by Mr. Lou Kratz and Mr. Ron Richburg. The authors also would like to thank Caroline Dawn Pulliam for her assistance with the planning and coordination of this study. Also deserving of thanks for their research and editorial support: Jinee Burdg, Master of Public Policy candidate and Sheetal Seewach, MS-Supply Chain candidate.

Bibliography

2010 U.S. Intellectual Property Enforcement Coordinator Strategic Plan. Executive Office of the President of the United States. February 2011. Accessed October 18, 2012. Available at http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_report_feb2011.pdf.

2011 U.S. Intellectual Property Enforcement Coordinator Strategic Plan. Executive Office of the President of the United States. June 2011. Accessed October 18, 2012. Available at www.iprcenter.gov/reports/ipr-center-reports/2011-joint.../file.

Accenture. "Keeping Ahead of Supply Chain Risk and Uncertainty." 2008. Available at http://www.oracle.com/us/products/applications/accenture-oracle-risk-pov-bwp-069959.pdf.

Aerospace AS5553 Resource Center. "What is AS5553?" 2009. Accessed October 18, 2012. Available at http://www.as5553.com/.

Aerospace Industries Association of America, Inc. "Counterfeit Parts: Increasing Awareness and Developing Countermeasures." Arlington, Virginia, March 2011. Accessed August 1, 2012. http://www.aia-aerospace.org/assets/counterfeit-web11.pdf.

Allianz Global Corporate & Specialty. "Global Supply Chains: The Growing Risks of Business and Supply Chain Interruption in Today's Interconnected World." March 2012. Accessed August 29, 2012 http://www.agcs.allianz.com/assets/PDFs/Special%20and%20stand-alone%20articles/Supply_Chain_Factsheet.pdf.

The Associated Press. "Toyota Car Production Plummets after Tsunami." Last modified April 25, 2011. Accessed September 27, 2012 http://www.usatoday.com/money/autos/2011-04-25-Toyota.htm.

Bartol, Nadya, Jon Boyens, Rama Moorthy, Celia Paulsen, and Stephanie Shankles. "Notional Supply Chain Risk Management Practices for Federal Information Systems." U.S. Department of Commerce: National Institute of Standards and Technology. Draft NISTIR 7622, March 2012. Available at http://csrc.nist.gov/publications/drafts/nistir-7622/second-public-draft_nistir-7622.pdf.

Brennan, Patrick. "Lessons Learned from the Japan Earthquake." Disaster Recovery Journal Summer 2011: 22-26. Accessed September 27, 2012 http://www.supplyrisk.com/Lessons_Learned_from_the_Japan_Earthquake.pdf.

Brintrup, Alexandra, et. al. "The Structure of the Toyota Supply Network: The Emergence of Resilience." CABDyN Working Paper # 2011-05-012 Received 16th May 2011, 8. Accessed November 1, 2012 http://www.cabdyn.ox.ac.uk/complexity_PDFs/Working%20Papers%202011/ToyotaRobustness.pdf.

Brunello, Brenda and Charles Robinson. "GSFC Supplier Assessments: Mitigating Risks through Corrective Action." NASA Safety Center. Presented October 18, 2011. Accessed October 22, 2012. Available at http://supplychain.gsfc.nasa.gov/sc2011b.brunelloc.robinsonasof1017.pdf.

Busch, Jason. "Toyota: Rebuilding and Fortifying a Global Supply Chain (Part 1)." Spend Matters. Last modified September 12, 2011 http://www.spendmatters.com/index.cfm/2011/9/12/Toyota-Rebuilding-and-Fortifying-a-Global-Supply-Chain-Part-1.

Closs, David, Cheri Speier, Judith Whipple, and M. Douglas Voss. "A Framework for Protecting Your Supply Chain." Logistics Management (Highlands Ranch, CO), September 2008. Accessed September 17, 2012. http://www.highbeam.com/doc/1G1-185243775.html.

Closs, David, Cheri Speier, Judith Whipple, and M. Douglas Voss. "Global Supply Chain Design Considerations: Mitigating Product Safety and Security Risks." Journal of Operations Management. 29(2011): 721-736.

Cornish, Paul, David Livingstone, Dave Clemente, and Claire Yorke. "On Cyber Warfare: A Chatham House Report." Chatham House (The Royal Institute of International Affairs). London, United Kingdom, November 2010. Available at http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf.

"Cyber Threats to National Security, Symposium One: Countering Challenges to the Global Supply Chain." Comments made by Stephen Chabinsky and Vergle Gipson. March 2, 2010. Available at http://asymmetricthreat.net/docs/asymmetric_threat_4_paper.pdf.

DeAngelis, Stephen F. Insights on Technology, Business and Government with a Focus on Supply Chain Management, Artificial Intelligence and Innovation blog.

DeAngelis, Stephen F. "Supply Chain Resilience and Supply Chain Security." Enterprise Resilience Management Blog, The. http://enterpriseresilienceblog.typepad.com/enterprise_resilience_man/2011/01/supply-chain-resilience-and-security.html.

Debolt, Paul A. and George W. Wyatt. "Real Parts: DOD Continues To Develop Policy On Counterfeit Electronic Parts." June 14, 2012. Available at http://www.venable.com/real-parts-dod-continues-to-develop-policy-on-counterfeit-electronic-parts-06-07-2012/.

Debs, Krystel. "Supply Chain Will be Ready by Autumn for Next Big Quake: Toyota." Saber blogosphere. http://saber-mena.com/blog/2012/03/supply-chain-will-be-ready-by-autumn-for-next-big-quake-toyota/.

"Defense Industrial Base Assessment: Counterfeit Electronics." U.S. Department of Commerce: Bureau of Industry and Security: Office of Technology Evaluation. January 2010. Accessed October 18, 2012. Available at http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf.

Defense Supply Center Columbus. "Criteria and Provisions for Qualified Suppliers List of Distributors (QSLD): FSCs 5961 (Semiconductors)/5962 (Microcircuits)." April 8, 2009.

Defense Supply Chain and Industrial Base Security Act, H.R. 344, 112th Congress 1st Session (2011).

E2open. "Going Global is Risky Business: Gain Better Control to Maintain Profitability." Foster City, California, November 2, 2009. Available at http://hosteddocs.ittoolbox.com/riskybizwp.pdf.

Ellison, Robert J., John B. Goodenough, Charles B. Weinstock, and Carol Woody, "Evaluating and Mitigating Software Supply Chain Security Risks." Carnegie Mellon: Research, Technology, and System Solutions (RTSS) and CERT Programs. May 2010. Available at http://www.sei.cmu.edu/reports/10tn016.pdf.

Enslow, Beth, "Stemming the Rising Tide of Supply Chain Risks: How Risk Managers' Roles and Are Changing Responsibilities." Report by MARSH, April 15, 2008. Available at http://usa.marsh.com/Portals/9/Documents/Stemming-the-Tide_final_4-16-08.pdf.

Escalante, Dr. Edgardo J. "Counterfeit Parts Training Module." Academy of Aerospace Quality. Accessed October 18, 2012. Available at http://aaq.auburn.edu/taxonomy/term/1.

Foley, Aaron. "Toyota Wants Better Communication in Supply Chain." WardsAuto. Last modified August 8, 2012. Accessed September 24, 2012 http://wardsauto.com/supply-chain/toyota-wants-better-communication-supply-chain.

Fong, E. Kenneth Hong. "Comprehensive Program Protection Planning." Presented at 14th Annual NDIA Systems Engineering Conference. San Diego, CA. October 25, 2011.

Foster, Steve. "Dryden Flight Research Center." NASA. Presented at Dryden Flight Research Center, 2012. Accessed October 4, 2012. Available at http://www.erai.com/presentations/General%20Session%201/NASA-Steve%20Foster.pdf.

Gottlieb, Craig, "Securing Goods Across the Supply Chain: Closing the Gaps in the Manufacturing Supply Chain to Achieve High Performance." Accenture, 2010. Accessed September 17, 2012. Available at http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Securing_Goods_Across_the_Supply_Chain.pdf.

Harrington, Lisa H. "Security Guard: Questions and Answers with Dennis Omanoff." *Inbound Logistics.* January 2012. Available at http://www.inboundlogistics.com/cms/article/security-guard-questions-and-answers-with-dennis-omanoff/.

Harrington, Lisa H, Sandor Boyson, and Thomas M. Corsi. "CISCO Case Study." *X-SCM: The New Science of X-treme Supply Chain Management*. New York: Routledge, 2011, 105-112.

Hearing on IT Supply Chain Security: Review of Government and Industry Efforts. March 27, 2012. Before United States House of Representatives Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, 112th Congress, 2nd Session. (statement of David Lounsbury, Chief Technology Officer, The Open Group). Accessed November 5, 2012. Available at http://www.hsdl.org/?view&did=704788.

Hearing on IT Supply Chain Security: Review of Government and Industry Efforts. March 27, 2012. Before United States House of Representatives Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, 112th Congress, 2nd Session. (statement of Mitchell Komaroff, Office of the Department of Defense Chief Information Officer). Accessed November 5, 2012. Available at http://www.hsdl.org/?view&did=704788.

Hearing on IT Supply Chain: Additional Efforts Needed by National Security-Related Agencies to Address Risks. March 27, 2012. Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives, 112th Congress, 2nd Session (statement of Gregory C. Wilshusen, Director Information Security Issues, United States Government Accountability Office). Accessed November 5, 2012. Available at http://www.gao.gov/assets/590/589617.pdf.

"Information Technology: Recommended Security Controls for Federal Information Systems and Organizations." National Institutes of Standards Technology. August 2009.

ISPE: International Leadership Forum. "Supply Chain Security: A Comprehensive and Practical Approach." Tampa, Florida. 2010.

Just-Auto Global News. "Toyota Rethinks Supply Chain Setup." Last modified March 29, 2012 http://asq.org/qualitynews/qnt/execute/displaySetup?newsID=13371.
Kelly, Michael P. "NASA/Goddard Space Flight Center. Supply Chain Management Program." Presented February 10-11, 2011 at PM Challenge. Accessed November 1, 2012 http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20110007132_2011005476.pdf.
Kendall, Frank III, Brett Lambert, and Zachary Lemnios. Prepared Statement. Presented to Senate Armed Services Subcommittee on Emerging Threats and Capabilities. May 3, 2011.
Kim, Chang-Ram. "RPT-UPDATE 4-Thai flooding impact spreads across world for Toyota." Reuters. Last modified October 27, 2011. Accessed September 24, 2012 http://www.reuters.com/article/2011/10/27/toyota-idUSL3E7LR00I20111027.
Kim, Chang-Ran. "Toyota Aims for Quake-Proof Supply Chain." Reuters. Last modified September 6, 2011. Accessed September 27, 2012 http://www.reuters.com/article/2011/09/06/us-toyota-idUSTRE7852RF20110906.
Kinaxis, Inc. "Essential Characteristics of a Supply Chain Risk Management Strategy." Supply Chain Expert Series. Ottowa, Ontario, June 2009. Accessed September 13, 2012. Available at http://www.kinaxis.com/whitepapers/Supply-Chain-Risk-Management-Strategy.cfm.
Kito, Tomomi, et. al. "The structure of the Toyota supply network: The emergence of Resilience." Working paper, May 16 2011. Accessed October 4, 2012 http://www.cabdyn.ox.ac.uk/complexity_PDFs/Working%20Papers%202011/ToyotaRobustness.pdf.
Langeland, Terje. "Sony, Toyota Shut Factories After Power Shortages Follow Earthquake Damage." Bloomberg, March 14, 2011. Accessed September 17, 2012 http://www.bloomberg.com/news/2011-03-14/toyota-sony-factories-shuttered-amid-earthquake-damage-power-shortages.html.
Lienert, Ana. "Resilient Auto Industry Reports Robust August Sales." Edmunds Inside Line. Last modified September 4, 2012. Accessed September 24, 2012 http://www.insideline.com/chevrolet/spark/resilient-auto-industry-reports-robust-august-sales.html.
Liker, Jeffrey K. The Toyota Way: 14 Management Principles from the World's Greatest Manufacturer. Madison, WI: McGraw-Hill, 2004.
Li, Ting and Qiongwei Ye. "New thoughts about Supply Chain Security after 9-11 Terrorist Attack." IEEE Explore, 978-1-4244-2013-1(2008): 2398 – 2399. Accessed September 17, 2012 http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04682937.
Livingston, Henry, Teresa Telesco, Lisa Gardner, Ric Loeslein, Ed Zelinski, and William Pumford. "Counterfeit Parts Safeguards and Reporting: U.S. Government and Industry Collaboration to Combat the Threat." *Defense Standardization Program Journal*. January/March 2010: 10, 13.
Livingston, Henry. "Securing the DOD Supply Chain from the Risks of Counterfeit Electronic Components: Recommendations on Policies and Implementation Strategy." BAE Systems Electronic Solutions. October 18, 2010.
Martin, Belva M. United States Government Accountability Office. "Rare Earth Materials in the Defense Supply Chain." April 1, 2010.
Martin, Belva. United States Government Accountability Office. "Defense Supplier Base DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of

Counterfeit Parts." GAO-10-389, March 2010. Available at http://www.gao.gov/assets/310/302313.pdf.
McMillan, Rob. "The Security Processes You Must Get Right." Research Paper. Feb 24, 2011.
Mojonnier, Tim. "Reducing Risk in the Automotive Supply Chain." Last modified March 18, 2011 http://businesstheory.com/reducing-risk-automotive-supply-chain-2/.
Mueller, Tracy. "Just-in-Time Production Dodges Disaster." Texas Enterprise. Last modified August 4, 2011 http://www.texasenterprise.utexas.edu/article/%E2%80%98just-time%E2%80%99-production-dodges-disaster.
Oltsik, Jon, Jennifer Gahm, and John McKnight. "Assessing Cyber Supply Chain Security Vulnerabilities within the U.S. Infrastructure." Enterprise Strategy Group. November 2010, 5-7, 13-19, 48-49.
The Open Group. "Industry Best Practices for Manufacturing Technology Products that Facilitate Customer Technology Acquisition Risk Management Practices and Options for Promoting Industry Adoption." Open Trusted Technology Provider Framework (O-TTPF™). Burlington, Massachusetts, February 2011. Available at https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?catalogno=W113.
The Open Group. "Open Trusted Technology Forum Overview v1.5." Presented by Open Trusted Technology Provider Framework (O-TTPF™). Accessed November 1, 2012. Available at http://www.opengroup.org/public/member/proceedings/q111/ottf_szakal.pdf.
Pelleg-Gillai, Barchi, Gauri Bhat, and Lesley Sept. "Innovators in Supply Chain Security: Better Security Drives Business Value." Stanford University: The Manufacturing Institute, July 2006.
Peters, Paul D. "Anti-Counterfeit." Presented to Product Support Manager's Conference by Deputy Assistant Secretary of Defense Supply Chain Integration. June 6, 2012.
Pinkerton Consulting and Investigations. "Risk Assessments and Risk Based Supply Chain Security." Accessed September 17, 2012. Presentation available at http://www.cosco-usa.com/omd/security/ctpat2010/2010-Seminar-Risk-Assessment-Training.pdf.
Pinkerton Consulting and Investigations, "Supply Chain Security in 21st Century." Accessed September 13, 2012. Presentation available at http://www.securitas.com/Global/Pinkerton/Supply%20Chain%20Security.pdf
Proctor, Paul E and Smith, Michael, "The Gartner Business Risk Model: A Framework for Integrating Risk And Performance." September 1, 2011.
QAD. "White Paper: Streamlining for Success: The Lean Supply Chain." Accessed September 17, 2012. Available at http://www.qad.com/Public/Documents/streamlining_for_success.pdf.
"QSLD Program (Qualified Suppliers List of Distributors)." Defense Logistics Agency, Land and Maritime, Sourcing and Qualifications. Accessed August 27, 2012. Available at http://www.landandmaritime.dla.mil/offices/sourcing_and_qualification/offices.aspx?section=QSL.

"Quake Still Rattles Suppliers." *The Wall Street Journal*. Last modified September 29, 2011. Accessed September 24, 2012 http://online.wsj.com/article/SB10001424053111904563904576586040856135596.html.

"Restarting Japan: A First Assessment June 2011 on the Road to Recovery After the Great East Japan Earthquake," (working paper, Swedish Agency For Growth Policy Analysis, Studentplan 3, SE-831 40 Östersund, Sweden, June 2011). http://www.tillvaxtanalys.se/tua/export/sv/filer/publikationer/working-paper-pm/WP_2011_15.pdf.

Ridge, Tom, Hon. "Cyber Threats to National Security: Countering Challenges to the Global Supply Chain." Presented at CACI & USNI Symposium, July 2010.

Root, Jonathon. "GSFC Supplier Assessments." Safety and Mission Assurance Directorate, Goddard Space Flight Center. October 18, 2011. Accessed October 22, 2012. Available at http://supplychain.gsfc.nasa.gov/sc2011j.rootasof1020.ppt.pdf.

Sadlovska, Viktoriya, Robert Shecterle, and Melissa Spinks. "Supply Chain Risk Management: Building a Resilient Global Supply chain." Aberdeen Group, July 2008. Available at http://www.cleartrack.com/content/content/Aberdeen_RISK.pdf.

"SAE AS5553: A New Standard in the Fight Against Counterfeit Electronic Parts." NASA Jet Propulsion Laboratory/California Institute of Technology. November 3, 2009. Accessed October 4, 2012. Available at http://www.dscc.dla.mil/downloads/psmc/Nov09/NewStdInFightAgainstCounterfeitElectronicParts.pdf.

SCDigest Editorial Staff. "Global Supply Chain News: Toyota Taking Massive Effort to Reduce its Supply Chain Risk in Japan." Supply Chain Digest. Last modified March 7, 2012. Accessed September 27, 2012 http://www.scdigest.com/ontarget/12-03-07-2.php?cid=5576&ctype=content.

Schmitt, Bertel. "'Enormous Delay in Delivery:' Toyota Production Back to Normal – By the End of the Year." Last modified April 22, 2011. Accessed September 27, 2012 http://www.thetruthaboutcars.com/2011/04/392463/.

Schmitt, Bertel. "Toyota Data Production Hit Hard in March." Last modified April 25, 2011. Accessed September 27, 2012 http://www.thetruthaboutcars.com/2011/04/toyota-production-data-hit-hard-in-march/.

Schreffler, Roger. "Quake Changes Little in Toyota's Supply Chain Strategy." *Wards Auto*. Last modified May 16, 2012. Accessed September 24, 2012 http://wardsauto.com/supply-chain/quake-changes-little-toyota-s-supply-chain-strategy-0.

Security Counterintelligence: Office of the National Counterintelligence Executive. "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011." October 2011. Available at http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

Sivcovich, Ken. "NASA Supplier Assessment Experience." DRS Sensors & Targeting Systems. Presented October 20, 2010. Accessed October 22, 2012. Available at http://supplychain.gsfc.nasa.gov/SC2010-K.Sivcovich.pdf.

Smith, Aaron. "Toyota's Woes: Lower Sales, Ratings Cut." CNN Money, last modified June 28, 2011 http://money.cnn.com/2011/06/28/news/international/toyota_earthquake/index.htm.

Steel, James. "Cisco." Presented at the Annual Global Conference, Council of Supply Chain Management Professionals, Atlanta, GA, September 2012.

Stephens, Kathryn, "Cyber Supply Chain." National Security Cyberspace Institute, Inc. (NSCI). November 18, 2010. Available at http://www.nsci-va.org/WhitePapers/2010-11-18-Cyber%20Supply%20Chain%20Whitepaper-Stephens.pdf.

Supply Chain Risk Leadership Council. "Supply Chain Risk Management: A Compilation of Best Practices." August 2011. Accessed September 13, 2012. Available at http://www.scrlc.com/articles/Supply_Chain_Risk_Management_A_Compilation_of_Best_Practices_final[1].pdf.

"Toyota Extends Cutback Due To Thailand Flooding." Krebs, Michelle, ed. Last modified November 4, 2011. Accessed September 24, 2012 http://www.autoobserver.com/2011/11/toyota-extends-cutback-due-to-thailand-flooding.html.

Toyota in the News. "Toyota Aims to Cut Production Costs by 20%." Last modified June 21, 2011. Accessed September 27, 2012 http://www.toyotainthenews.com/toyota-aims-to-cut-production-costs-by-20/.

"The Toyota Motor Corporation." Chawalit Jeenanunta Research Group. Last modified August 25, 2009. Available at http://chawalit.siit.tu.ac.th/doku.php?id=seniorprojects:2009:report_marvellous:toyota_motor_corporation.

Toyota Motor Corporation Annual Report 2012. Accessed September 24, 2012 http://www.toyota-global.com/investors/ir_library/annual/pdf/2012/

Toyota. "TMC Announces Results for April 2011." Last modified May 27, 2011. Accessed September 27, 2012 http://www2.toyota.co.jp/en/news/11/05/0527.html.

Toyota. "Worldwide Operations." Accessed September 24, 2012 http://www.toyota-global.com/company/profile/overview/in_the_world/.

"Understanding Supply Chain Risk Matrices: Risk can be Analyzed Using Several Types of Tools; HP Matches Risk Areas with Supply Chain Processes." Supply Chain Digest Editorial Staff. Supply Chain Digest, July 13, 2008.

United States Department of Commerce: Bureau of Industry and Security: Office of Technology Evaluation. "Defense Industrial Base Assessment: Counterfeit Electronics." January 2010. Available at http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf.

United States Department of Defense: OUSD(AT&L) Systems and Software Engineering/Enterprise Development. "Risk Management Guide for DOD Acquisition, Sixth edition." August 2006. Available at http://www.acq.osd.mil/se/docs/2006-RM-Guide-4Aug06-final-version.pdf.

United States Government Accountability Office. "National Security – Related Agencies Need to do Better." GAO-12-361, March 2012. Available at http://www.gao.gov/assets/590/589568.pdf.

Wally, Buran. "Supply Chain: Toyota's Quarterly Profit Slides on Earthquake." Firestorm (blog). http://blog.firestorm.com/2011/05/16/hello-world/.

Wieland, Andreas. "Strategic Supply Chain Security." Journal of Homeland and Security (2009).

Wilcutt, Terry and Wilson B. Harkins. "Counterfeit Electronic Parts." Presented at NASA Leadership ViTS Meeting, May 2012. Accessed October 4, 2012. Available at http://nsc.**nasa**.gov/SFCS/SystemFailureCaseStudyFile/Download/257/.

Wilkerson, Taylor. "Governing Tangible Risk – The SCOR Model." In The New Science of X-treme Supply Chain Management, edited by Lisa H. Harrington, Dr. Sandor Boyson, and Dr. Thomas M. Corsi, 95-103. New York: Taylor & Francis, 2011.

Wilshusen, Gregory C. United States Government Accountability Office. "IT Supply Chain: National Security-Related Agencies Need to Better Address Risks." March 2012. Accessed November 5, 2012. Available at http://www.gao.gov/assets/590/589568.pdf.

World Economic Forum. "New Models for Addressing Supply Chain and Transport Risk." Geneva, Switzerland, 2012. Accessed August 1, 2012. Presentation available at http://www.weforum.org/reports/new-models-addressing-supply-chain-and-transport-risk.

Zolli, Andrew. "Resilience Strategies for a Volatile World." Harvard Business Review (blog). http://blogs.hbr.org/ideacast/2012/07/resilience-strategies-for-a-vo.html.

Zulueta, Phil. "Counterfeit Electronics: NASA Update." NASA Jet Propulsion Laboratory and California Institute of Technology. Presented June 29, 2011. Accessed October 18, 2012. Available at http://nepp.nasa.gov/workshops/etw2012/submissions/talks/Wednesday/1130%20-%20Counterfeit%20Electronics%20-%20NASA%20Update.pdf.

Zulueta, Phil. "Industry Game Changers: SAE G-19 Standards Updates." Presented May 17, 2012 at ERAI Executive Conference. Accessed October 4, 2012. Available at http://www.erai.com/presentations/General%20Session%201/Industry%20Game%20Changes%20-%20Phil%20Zulueta.pdf.

Zulueta, Phil. "SAE International Releases Standard AS5553 - Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition." NASA Jet Propulsion Laboratory. Accessed October 18, 2012. Available at http://www.pacs.arizona.edu/files/S021306_Reference_Document_AS5553.pdf.

About the Authors

Jacques S. Gansler

The Honorable Jacques S. Gansler, former Under Secretary of Defense for Acquisition, Technology, and Logistics, is a Professor and holds the Roger C. Lipitz Chair in Public Policy and Private Enterprise in the School of Public Policy, University of Maryland; he is also the Director of both the Center for Public Policy and Private Enterprise and the Sloan Biotechnology Industry Center. As the third-ranking civilian at the Pentagon from 1997 to 2001, Professor Gansler was responsible for all research and development, acquisition reform, logistics, advance technology, environmental security, defense industry, and numerous other security programs.

Before joining the Clinton Administration, Dr. Gansler held a variety of positions in government and the private sector, including Deputy Assistant Secretary of Defense (Material Acquisition), assistant director of defense research and engineering (electronics), senior vice president at TASC, vice president of ITT, and engineering and management positions with Singer and Raytheon Corporations.

Throughout his career, Dr. Gansler has written, published, and taught on subjects related to his work. Gansler recently served as the Chair of the Secretary of the Army's "Commission on Contracting and Program Management for Army Expeditionary Forces." He is also a member of the National Academy of Engineering and a Fellow of the National Academy of Public Administration. Additionally, he is the Glenn L. Martin Institute Fellow of Engineering at the A. James Clarke School of Engineering, an Affiliate Faculty member at the Robert H. Smith School of Business, and a Senior Fellow at the James MacGregor Burns Academy of Leadership (all at the University of Maryland). From 2003–2004, he served as Interim Dean of the School of Public Policy. From 2004–2006, Dr. Gansler served as the Vice President for Research at the University of Maryland.

William Lucyshyn

William Lucyshyn is the Director of Research and a Senior Research Scholar at the Center for Public Policy and Private Enterprise in the School of Public Policy, University of Maryland. In this position, he directs research on critical policy issues related to the increasingly complex problems associated with improving public-sector management and operations and with how government works with private enterprise. Current projects include modernizing government supply-chain management, identifying government sourcing and acquisition best practices, and analyzing Department of Defense business modernization and transformation. Previously, Mr. Lucyshyn served as a program manager and the principal technical advisor to the Director of the Defense Advanced Research Projects Agency (DARPA) on the identification, selection, research, development, and prototype production of advanced technology projects.

Prior to joining DARPA, Mr. Lucyshyn completed a 25-year career in the U.S. Air Force. Mr. Lucyshyn received his Bachelor degree in Engineering Science from the City University of New York and earned his Master's degree in Nuclear Engineering from the Air Force Institute of Technology. He has authored numerous reports, book chapters, and journal articles.

Lisa H. Harrington

Lisa H. Harrington holds a research appointment to the Center for Public Policy and Private Enterprise at the University of Maryland's School of Public Policy, where her research focus is on defense supply chain management. She is Associate Director of the Supply Chain Management Center at the Robert H. Smith School of Business University of Maryland, and a faculty lecturer there. Ms. Harrington served as lead author on the recently published book, X-SCM: The New Science of X-treme Supply Chain Management (2010), and co-authored two other books, In Real Time: Managing the New Supply Chain (2004), and Logistics and the Extended Enterprise: Benchmarks and Best Practices for Manufacturing Professionals (1999).

Ms. Harrington has consulted in the field of supply chain management for more than 20 years, serving clients in both the public and private sectors. She is a former board member of the Council of Supply Chain Management Professionals and the Warehousing Education & Research Council. She earned her Bachelor of Arts degree in communications from Brown University, and holds an Executive Education Certificate in Logistics Management from Michigan State University.

Appendix

Defense Supply Center Columbus. "Criteria and Provisions for Qualified Suppliers List of Distributors (QSLD): FSCs 5961 (Semiconductors)/5962 (Microcircuits)." (April 8, 2009).

1.0 INTRODUCTION

Qualification for placement on the Qualified Suppliers List for Distributors (QSLD), and the maintenance of QSLD status, requires the distributor to demonstrate that it has in place, and uses on a continuous basis, a Quality Management System (QMS) that meets the criteria set forth in JESD31 and complies with the provisions and clauses of each solicitation/contract or purchase order for items in FSCs 5961 and 5962. The objective of the QSLD Program is to ensure that the distributor continuously controls its processes to provide consistent delivery of products that conform to the contract/purchase order specification requirements. Four key elements are required of distributors who wish to be listed on the QSLD and to maintain QSLD status. These are:

a. The distributor must have evidence of using a documented Quality Management System which meets DLA's criteria;

b. The distributor must have on hand and maintain evidence that (1) the QPL/QML products supplied were produced by a Manufacturer whom is listed (or was at date of manufacture) on the QPL or QML; (2) commercial products were produced by the specified original manufacturer (to include information tracing the product back to the specified source); and (3) products procured from another distributor are from a distributor or through a chain of distributors each listed as an approved QSLD supplier. All products pursuant to DLA's contract/purchase order requirements for items in FSCs 5961 and 5962 must be obtained from, or flow through QSLD providers, with an unbroken chain of traceability documentation back to the OEM. This closed loop flow must be supported by the provider's traceability documentation. No deviations are permitted under this QSLD program;

c. The distributor must have and maintain evidence that product is not commingled and lot identity has been maintained; and

d. The distributor must have and maintain evidence that the quality of the product is not altered by Distributors.

2.0 SCOPE

The products DLA procures which are included in this program are certain safety critical and high reliability items which fall into the Federal Supply Classes of 5961 (semiconductors) and 5962 (monolithic and hybrid microcircuits). See

http://www.landandmaritime.dla.mil/Programs/MilSpec/DocSearch.asp to obtain specifications and standards.

2.1 OBJECTIVE

2.1.1 The objective of the QSLD Program is to establish and maintain a list of pre-qualified Distributors whose regular use of in-place process controls is designed to ensure delivery of quality products that meet specified requirements, and that participant Distributors likewise control all applicable value-added inventory services associated with defense logistics. The ultimate goals are to improve quality with quality system elements and to reduce product delivery lead times by means of standard quality/process control practices in lieu of certain Government quality assurance provisions, source inspections, and product verification testing (PVT).

2.1.2 Candidate business distributors are approved for these lists by complying with an established set of quality management and process control requirements, and agreeing to a set of administrative requirements. This Criteria and Provisions document contains these requirements, and is based upon the best commercial business practices for quality control and customer satisfaction.

2.1.3 Distributors ultimately approved for listing under one or more DLA QSLD program(s) agree, as a condition of continued Qualification, to continuously maintain their process controls at a level sufficient to meet the QSLD Criteria requirements for all qualified commodities and remain compliant with the key elements set forth under Section 1.0, Introduction, above. Evidence of non-compliance with any of the QSLD Criteria requirements or the key elements under Section 1.0 may be cause for immediate removal.

Toyota Appendix[158]

Figure 35: Toyota Plants in Japan

	Name	Main products	Start of operations	Unit production (1 = 1,000 vehicles)	Number of employees
①	Honsha Plant	Forged parts, hybrid system parts, chassis parts	Nov. 1938	-	4,133
②	Motomachi Plant	Crown, Mark X, Estima, LFA	Aug. 1959	62	7,273
③	Kamigo Plant	Engines	Nov. 1965	-	3,124
④	Takaoka Plant	Corolla, iQ	Sept. 1966	131	3,112
⑤	Miyoshi Plant	Transmission-related parts, forged parts, engine-related parts	July 1968	-	1,483
⑥	Tsutsumi Plant	Prius, Camry, Premio, Allion, Scion tC	Dec. 1970	388	5,134
⑦	Myochi Plant	Powertrain-related parts	June 1973	-	1,549
⑧	Shimoyama Plant	Engines, turbochargers, catalytic converters	March 1975	-	1,739
⑨	Kinu-ura Plant	Transmission-related parts	Aug. 1978	-	3,027
⑩	Tahara Plant	LS, GS, IS, GX, RAV4, Wish, Land Cruiser, Vanguard, engines	Jan. 1979	322	8,089
⑪	Teiho Plant	Mechanical equipment, moldings for resin and casting and forging	Feb. 1986	-	1,102
⑫	Hirose Plant	Research and development and production of electronic control devices, ICs	March 1989	-	1,589
●	TOYOTA MOTOR KYUSHU, INC.	IS, ES, HS, CT, RX, SAI, Harrier, Highlander, engines, hybrid system parts	Dec. 1992	291	7,164
●	TOYOTA MOTOR HOKKAIDO, INC.	Transmissions, Powertrain-related parts	Oct. 1992	-	2,320
●	TOYOTA MOTOR EAST JAPAN, INC.	Corolla, Aqua, Isis, Ractis, ist, Century, Comfort, Powertrain-related parts	July 2012	-	7800
●	TOYOTA AUTO BODY CO., LTD.	Prius, Estima, Hiace, Noah, Voxy, Alphard, Vellfire, Land Cruiser, Coaster	Aug. 1945	541	11,622

1. As of December 2011

[158] Toyota. "Worldwide Operations." Accessed September 24, 2012 http://www.toyota-global.com/company/profile/overview/in_the_world/.

The Center for Public Policy and Private Enterprise provides the strategic linkage between the public and private sector to develop and improve solutions to increasingly complex problems associated with the delivery of public services — a responsibility increasingly shared by both sectors. Operating at the nexus of public and private interests, the Center researches, develops, and promotes best practices; develops policy recommendations; and strives to influence senior decision-makers toward improved government and industry results.

The Center for Public Policy and Private Enterprise is a research Center within the University of Maryland's School of Public Policy.