SYM-AM-17-084

Proceedings
of the
Fourteenth Annual Acquisition Research Symposium

Thursday Sessions
Volume II

Acquisition Research:
Creating Synergy for Informed Change

April 26–27, 2017

Published March 31, 2017

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

Acquisition Research Program
Graduate School of Business & Public Policy
Naval Postgraduate School

Making Smart Decisions About Supply Chain Security in the Age of Globalization

Elizabeth McDaniel—PhD, a Research Staff Member at the Institute for Defense Analyses (IDA) for five years, has focused her efforts on education and awareness of supply chain risk, cyber workforce development, and higher education opportunities for DoD personnel. Prior to IDA, Dr. McDaniel spent her career at institutions of higher education, including National Defense University, as a professor, scholar, and leader. [emcdanie@ida.org]

Michelle Albert—has been a Research Associate at IDA for over three years and serves as a researcher, technical writer, and editor. Her research at IDA has covered a range of topics, including supply chain security and risk management education and awareness. [malbert@ida.org]

Brian Cohen—PhD, has been a Research Staff Member in the Information and Technology Systems Division of IDA for 30 years. Dr. Cohen has performed a range of studies at IDA, with a focus on technology, policy, and business assessments for national security. Recent studies have examined problems with assuring the electronics supply chain for defense systems in the face of increased trends toward offshore sources. [bcohen@ida.org]

Catherine J. Ortiz—is the founder of Defined Business Solutions LLC. She manages the outreach activity for the DoD's Trusted Foundry Program and serves as the Vice Chair of the National Defense Industrial Association's (NDIA's) Manufacturing Division's Supply Chain Network Committee. [cjortiz@definedbusiness.com]

Abstract

Over the last two decades, the Department of Defense (DoD) became increasingly concerned about supply chain security as the supply chain for products became increasingly dependent on commercial and global sources. Supply chains, which are interconnected webs of people, processes, technology, information, and resources around the world, are creating serious asymmetrical threats to our national defense and warfighting capabilities. Hardware- and software-enabled components that traverse these global supply chains afford our adversaries cyberattack vectors that can compromise weapon systems. Educating and enabling the acquisition community to competently assess and make risk decisions in this new area is a particular challenge. Recent education, training, and awareness efforts seek to illuminate a narrow, deeply technical subject such that acquisition professionals can make cost-effective decisions. To that end, this paper presents a new framework for assessing the supply chain risk of particular components while complying with policies and regulations and staying within budget.

Introduction

Electronic components are essential to the Department of Defense's (DoD's) business equipment, communications networks, weapons systems, and supporting platforms. These electronic components follow complex paths, from design, through multiple manufacturing steps, to final test and delivery. The journey that components take through organizations and locations is commonly referred to as a supply chain. Understanding and managing the risks of using components from these generally commercial and global supply chains presents unique challenges for the DoD and its contractors. Attacks by nation-states and other organized groups using the global information and communications technology

(ICT)[1] supply chain can result in service disruption, insertion of malicious functionality, data exfiltration, and intellectual property theft. Supply chain security is imperative for the DoD and other government organizations, as well as many private sector entities. The goal of supply chain security is to reduce a component's or system's susceptibility to supply chain threats[2] and reduce or mitigate the potential impact of any such exploitation.

This paper provides an overview of the risks associated with the global supply chain for the products and systems that power our machines, computer applications, weapons, and vehicles. Threats and vulnerabilities associated with the supply chain create risks that have the potential to affect the performance and security of the components themselves and the systems in which they are integrated. Becoming aware of the risks is the first step; responding appropriately to ensure security, which varies according to one's role in an organization, is the second. Appropriate education, training, and awareness (ETA) and risk mitigation tools must be available for each role. This paper describes the threats and challenges associated with supply chain security and response. The paper capitalizes on the results of an informal survey of current supply chain ETA efforts and offers a new decision-making tool for supply chain security, the Trustworthy Supplier Framework. The evolution and adoption of this new decision-making tool will depend on collaboration across sectors to increase awareness of the problem and to educate and train key personnel across the government, research, and industry communities.

In this paper, *supply chain security* refers to the security and integrity of a component as it travels along its supply chain. *Supply chain risk management (SCRM),* historically considered a logistics-based discipline, focuses on the movement of the component through its supply chain and the threats to this movement, such as earthquakes. The DoD now uses the term *SCRM* in acquisition to refer to the threat of malicious actors who seek to intervene in the supply chain to impair the security of DoD systems and missions. In this paper, the term *SCRM* is reinterpreted and refers to the processes needed to ensure that components are protected against these malicious actors. Much of the policy and guidance discussed in this paper uses *SCRM* in this security context. Both terms are used in this paper, *and supply chain security* and *SCRM* should be considered synonymous and focused on protection against malicious actors.

Supply Chain Security in the Age of Globalization Essentials

Overview of the Benefits and Challenges of Global Supply Chains

The DoD depends on the best and most reliable ICT to build powerful and complex systems. Large systems typically contain thousands of ICT components that are used for

---

[1] ICT is technology used for gathering, storing, retrieving, and processing information. ICT includes microelectronics, printed circuit boards, computing systems, software, signal processors, mobile devices, satellite communications, and networks. The term ICT reflects the convergence of information technology (IT) and communications; it is not restricted to IT. (IT is defined as any system or equipment "used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data" [40 U.S.C. § 11101].)

[2] Throughout this paper we use the term *threats* to refer to nation-state, terrorist, criminal, or other organized actors. Historical supply chain threats such as earthquakes and trucker strikes are also within the scope of threats as used in this paper.

gathering, storing, retrieving, transmitting, and processing information. They include components internal to a system, such as microelectronics, printed circuit boards, computing systems, software, and signal processors, as well as end devices and complete systems, such as mobile devices, satellites, and their networks.

Today, most of the ICT components used in DoD systems and networks are obtained from commercial sources. These commercial products take advantage of global talent, resources, and manufacturing capabilities, resulting in products that typically can be purchased at lower cost than ICT components that are custom-developed for the DoD. Globalization, however, while affording these advantages, creates complex global supply chains that are often opaque and difficult to trace, which creates security challenges. Products traverse national borders and independent companies many times on their way to their point of integration into DoD systems or networks and the end user.

These complex supply chains provide adversaries with a large attack surface within which they can attempt to tamper with, modify, or influence products. The goal of supply chain security is to reduce a component's or system's susceptibility to supply chain attacks and limit any potential impact. Attacks on defense supply chains can occur throughout the DoD system development life cycle,[3] and through multiple entry points. There are entry points for exploitation, manipulation, and counterfeit insertion during component design, manufacturing, testing, transport, delivery, installation, repair, and upgrade.

It is not possible to anticipate or eliminate all vulnerabilities in systems and components, so security risks must be managed and mitigated. And, because everything is connected today, a single exploited ICT component in a DoD system or network can not only affect that system but multiple systems today and in the future. As such, it is imperative to consider the risks associated with each ICT component that is integrated into a system.

Current Guidance for Global Supply Chain Security

Taking action to ensure supply chain security starts with recognizing the threats and vulnerabilities associated with the ICT supply chain, assessing the risks posed by those threats and vulnerabilities, and determining how to manage the assessed risks. When adversaries are successful in their efforts to tamper with ICT components, supply chain attacks create cybersecurity risks that affect a system's confidentiality, integrity, and availability. Supply chain exploitation, a relatively new aspect of cybersecurity, requires the attention of personnel across the system development life cycle, some of whom may be unaware of their critical roles in securing DoD networks and systems.

---

[3] In this document (as well as IDA's ICT SCRM awareness module; see the section titled *IDA's ICT Global Supply Chain Risk Management Awareness* Module for more information), components and systems obtained through simple procurement or as part of the Defense Acquisition Management System (DAMS) are described as having *system development life cycles* from design to disposal. The Joint Capabilities Integration Development System (JCIDS) process is referred to as the *requirements phase.* Some of the DAMS phases have been combined and renamed here for ease of understanding. The *acquisition phase* refers to component and system design, development, testing, production, and deployment; the *operations and sustainment phase* refers to component and system operations and support (including repair or upgrade); and the *disposal phase* refers to the disposal of the component and system.

The DoD recognizes the significance of the threat and is expanding its strategy, articulating new policies, and instituting processes for acquisition, cybersecurity, and risk management to manage ICT global supply chain risk across the system development life cycle. Actions taken in response to supply chain risk will vary depending on the criticality of the system and component and the phase of the life cycle.

Relevant DoD Instructions, Directives, and Regulations

DoD Instruction (DoDI) 5200.39*, Critical Program Information (CPI) Protection Within Research, Development, Test, and Evaluation (RDT&E),*[4] and DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)* (DoD CIO & USD[AT&L], 2012), focus on threats to technology and threats to components, respectively. For protecting CPI, the policy provides guidance to mitigate CPI exploitation; extend operational effectiveness of military systems through the application of appropriate risk management strategies; employ the most effective protection measures, including system assurance and anti-tamper (AT); and document these measures in a Program Protection Plan (PPP). The enclosure on systems engineering in DoDI 5000.02, *Operation of the Defense Acquisition System* (USD[AT&L], 2015), articulates the PPP processes.

The DoD TSN strategy identifies program protection and information assurance implementation as essential to the development of uncompromised weapons and information systems. The strategy strives to integrate robust systems engineering, SCRM, security, counterintelligence, intelligence, information assurance, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust. The purpose of DoDI 5200.44 is to minimize the risk that warfighting capability will be impaired due to vulnerabilities in system design or to subversion of mission-critical functions or components. It focuses on mission-critical systems and critical components and suggests risk management processes, tools, and techniques to reduce vulnerabilities, control quality, reduce and mitigate the likelihood of using products containing counterfeit or malicious functions, and increase the traceability of critical components. Systems Security Engineering (SSE), a specialty discipline within systems engineering, supports the development of programs and design-to-specifications that provide life-cycle protection for critical defense resources. The primary vehicle for integrating systems security engineering into systems engineering processes during the system development life cycle is program protection planning. Programs perform criticality analysis to identify their systems' mission-critical functions and components; assess threats, vulnerabilities, risks, and impacts; and select and apply countermeasures and mitigations.

DoDI 8500.01, *Cybersecurity*, instructs the DoD to implement a multi-tiered risk management process that encompasses supply chain risks associated with global sourcing and distribution, weakness or flaws inherent to IT, and vulnerabilities introduced through

[4] The DoD defines *CPI* as "elements or components of a research, development, and acquisition (RDA) 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." CPI includes information about applications, capabilities, and processes and elements or components critical to military system or network mission effectiveness (USD[I] & USD[AT&L], 2015).

faulty design, configuration, or use that will be managed, mitigated, and monitored as appropriate (DoD CIO, 2014a).

DoDI 8510.01, Ri*sk Management Framework (RMF) for DoD Information Technology (IT),* provides the DoD with an integrated, enterprise-wide decision structure for cybersecurity risk management (DoD CIO, 2014b). The framework, captured in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (NIST, 2010), seeks to improve information security, strengthen risk management processes, and encourage reciprocity among federal agencies. Components, Services, and Agencies are responsible for resourcing RMF implementation. The RMF informs acquisition processes for information technology (IT) and applies to all DoD IT that receives, processes, stores, displays, or transmits DoD information, including information systems (IS); weapons systems; command, control, communications, computers, and intelligence (C4I) systems; sensor systems; and other platform IT (PIT) systems.

The *DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) Into the System Development Life Cycle* is intended to help program managers integrate cybersecurity into their systems in accordance with the RMF and DoD policy (DoDI 8510.01, 8500.01, 5000.02).

DoDI 5000.02, *Operation of the Defense Acquisition System*, which states the processes and policies for governing the Defense Acquisition System, was updated on February 2, 2017, to include an enclosure on "Cybersecurity in the Defense Acquisition System" (USD[AT&L], 2015). This enclosure discusses a range of cybersecurity risks to DoD systems and networks and assigns program managers responsibility for the cybersecurity of their programs, systems, and networks. The enclosure outlines activities for mitigating cybersecurity risks, including safeguarding program information against a cyberattack, designing and developing systems that can operate in cyber threat environments, and program protection planning. It also discusses specific actions to implement during the materiel life cycle (by phase) and lists resources for performing cybersecurity and related program security activities.

Relevant NIST Publications

In 2017, NIST updated its *Framework for Improving Critical Infrastructure Cybersecurity*, Draft Version 1.1 (referred to as the Cybersecurity Framework), to include cyber supply chain risk management (cyber SCRM). The Cybersecurity Framework provides organizations with a means of identifying and describing their current cybersecurity posture and their target state for cybersecurity, identifying and prioritizing opportunities for moving toward that target state, assessing their progress, and communicating internally and externally about cybersecurity risk. The Framework has three parts: the Framework Core, a set of cybersecurity activities and outcomes; Framework Implementation Tiers, which characterize an organization's cybersecurity risk management practices; and the Framework Profile, which aligns an organization's risks and needs with standards and guidelines (NIST, 2017).

The Cybersecurity Framework identifies communicating cybersecurity requirements to stakeholders as one aspect of cyber SCRM. Another is identifying, assessing, and mitigating products and services that may be compromised or counterfeit, or are vulnerable to malicious tampering. Cyber SCRM activities include determining cybersecurity requirements for suppliers, enacting cybersecurity requirements in contracts, communicating how the requirements will be validated and verified, and determining whether the requirements are met (NIST, 2017).

NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (Boyens et al., 2015), adapts the controls listed in SP 800-53, *Security and Privacy Controls for Federal Information Systems* (NIST, 2013), to SCRM. SP 800-161 provides federal agencies with guidance on assessing and implementing risk management processes and controls to manage ICT supply chain risks. It describes ICT SCRM as sitting at the intersection of security, integrity, resilience, and quality. Security refers to information confidentiality, availability, and integrity; integrity refers to the confidence that an ICT product is genuine and will perform as expected; resilience refers to ensuring the ICT supply chain will provide needed products under stress; and quality refers to reducing vulnerabilities in products that may lead to component or system failure or may provide an avenue for exploitation.

SP 800-161 provides ICT SCRM guidance at the organization, mission/business-process, and information-system levels, and it recommends that organizations build their ICT SCRM processes on a foundation of standardized SCRM practices. SP 800-161 covers more than supply chain security and SCRM, but it focuses on information assurance controls. An organization's ICT SCRM plan should focus on managing risk and be able to adapt to threats, respond to internal changes, and adjust to the rapid change inherent to the commercial sector's ICT supply chains. SP 800-161 presents a catalog of 236 controls divided into 17 families: Access Control, Awareness and Training, Audit and Accountability, Security Assessment and Authorization, Configuration Management, Contingency Planning, Incident Response, Maintenance, Media Protection, Planning, Program Management, System and Services Acquisition, Personnel Security, Provenance, Risk Assessment, System and Communication Protection, and System and Information Integrity (NIST, 2010).

NIST SP 800-161 serves as the foundation for the emerging Trustworthy Supplier Framework that is highlighted later in this paper.

Education, Training, and Awareness

The Imperative for Supply Chain Security Education, Training, Awareness, and Guidance

One challenge in addressing security risks associated with global supply chains is to increase awareness of these risks and prepare the system development life-cycle workforce to assess risk and make effective mitigation decisions and actions. Supply chain risk cannot be eliminated—it must be managed. Managing supply chain risk requires personnel who have roles in the life cycle of systems and components, as well as employees of prime contractors and their suppliers, to be aware of supply chain risks, their relevance to their roles, and appropriate responses.

Education, training, and *awareness* are terms that are often used interchangeably and incorrectly. They pertain to different purposes, time horizons, and methods that rely on learning. Efforts to increase *awareness* seek to focus attention on a topic by presenting facts and issues in a manner meant to generate interest and desire for further learning and to shift thinking or level of concern. Awareness efforts include live briefings, online activities, posters and fliers, and articles. *Training*, which is functional and focused on the "how to" aspect, is designed to change behavior by developing specific skills or competencies.

Training outcomes are typically well articulated so that learners know what is expected of them and at what level of proficiency. *Education* is conceptual, strategic, and future-focused. Education seeks to enhance critical and creative thinking and to develop depth and breadth of understanding of principles, concepts, and ideas and their application in novel situations.[5]

In addition to the awareness, training, and education activities that are advancing action in support of supply chain security, a fourth activity, *guidance*, involves experts, researchers, and practitioners sharing and refining standards and best practices. When ETA is used in the remainder of this paper, it includes guidance.

IDA's ICT Global Supply Chain Risk Management Awareness Module

With the sponsorship of the DoD Chief Information Officer's (CIO's) supply chain security effort, IDA developed the ICT Global Supply Chain Risk Management Awareness module in 2014 (McDaniel, Barth, & Albert, 2014). It presents an overview of ICT supply chain exploitation and its potential risk to the DoD, and it summarizes the current array of responses. It is designed to promote awareness of the risks inherent to the ICT global supply chain and to increase understanding of ICT SCRM. The module was designed for DoD personnel and others with responsibility for oversight, risk management, program management, budget, acquisition, system design and development, security, operations, test and evaluation, and system audit. The module leverages available products and processes to allow users to update and modify the content to fit their purpose and audience. IDA developed the content in part through interactions with experts and stakeholders participating in the DoD Trusted Systems and Networks (TSN) Roundtable, a community of representatives from DoD departments and agencies interested in developing and sharing TSN requirements and best practices.

Traditionally, the term *SCRM* primarily refers to logistics, which deals with packaging and delivering products from the manufacturing site to the purchaser. But mastery of logistics does not necessarily equal or include security. ICT SCRM, as defined in IDA's module, refers to the process of identifying critical components and functions, vulnerabilities, and threats to the supply chain, and developing strategies to respond. It focuses on the security and integrity of the products traversing the supply chain, not just how the products traverse the supply chain. The module, which covers SCRM throughout the system development life cycle, is organized around three themes:

1. The New Insider Threat Is Not a Person—It's ICT;
2. Supply Chain Risk Is a Condition to Be Managed, Not a Problem to Be Solved;
3. Take Action to Manage Global Supply Chain Risk.

The module is designed to prompt DoD personnel to care, think, and act in response to the real risks that result from the supply chains of ICT products across the life cycle. The module is available for public release on DVD and comprises an introductory video, a comprehensive narrative report, an accompanying slide set, and a source document repository. The four-minute video is available on the IDA website at https://www.ida.org/SAC/SACResearchDivisions/ITSD/ITSD_Ideas_Home.aspx.

[5] These definitions are adapted from NIST SP 800-16 (April 1998).

The New Insider Threat Is Not a Person—It's ICT

Theme 1 identifies the elements of supply chain security and explains the national security risks associated with global supply chain exploitation. Most of the ICT components used in DoD systems and networks today are obtained from commercial sources and traverse global supply chains that are often opaque and difficult to trace.

As an ICT component traverses its supply chain, it passes from country to country, company to company, and person to person. Each company has its own logistics security standards, and ICT components are often stored or transported in ways that leave them open to tampering and attack. Supply chain attacks can occur throughout the DoD system development life cycle; entry points for exploitation and manipulation include component design, manufacturing, transport, delivery, installation, and repair or upgrade.

Such attacks can result in disruption of service, insertion of malicious functionality, data exfiltration, and theft of intellectual property. The goal of supply chain security is to reduce a component's or system's susceptibility to supply chain threats and the potential impacts of those threats.

Supply Chain Risk Is a Condition to Be Managed, Not a Problem to Be Solved

Theme 2 explains why supply chain risk must be managed, discusses the key concepts of risk management in the context of ICT SCRM, and offers a range of responses to identified risks. Given the generally complex and opaque supply chains of many critical components from commercial sources, it is impossible to remove risk entirely, and attempting to do so can be extremely expensive. Actively managing risk must be considered for every ICT component purchased or integrated into a system. Limits on time and money require the DoD to focus on risks to mission-critical functions, which are functions that, if compromised, could degrade a system's ability to meet its core mission.

If the assessed risk is high, the DoD has four basic responses: treat it, tolerate it, transfer it, or terminate it. Treating the risk means applying countermeasures and mitigations to lessen the consequence of a compromised component or system by incorporating risk management strategies throughout a component or system's life cycle.[6] Transferring, tolerating, or terminating the risk should be considered if it is better to treat the risk at a later time, if there are insufficient resources to treat it now, or if available treatment options do not reduce the risk to an acceptable level. Options to consider in response to an identified risk range from doing nothing, which entails no effort or extra costs up front, to redesigning a system to avoid using a component with unacceptable risk mitigation options, which involves more effort and higher costs.

Take Action to Manage Global Supply Chain Risk

Theme 3 describes the current complex, dynamic, and evolving environment of relevant government and DoD policies, standards, and strategies that guide the management of supply chain risk across the phases of the system development life cycle.

---

[6] According to the Joint Doctrine, *countermeasures* are devices or techniques applied to impair the operational effectiveness of adversary activity. In the context of ICT SCRM, countermeasures prevent adversaries from exploiting supply chain or component vulnerabilities. Mitigations are actions taken to alleviate the risks or effects resulting from vulnerabilities in critical components or systems (*DOD Dictionary of Military and Associated Terms*, 2017).

The DoD has articulated requirements in acquisition policy (DoDI 5000.02, *Operation of the Defense Acquisition System,* and DoDI 5200.44, P*rotection of Mission Critical Functions to Achieve Trusted Systems and Networks [TSN*]), and in cybersecurity policy (DoDI 8500.01, *Cybersecurity*, and DoDI 8510.01, *Risk Management Framework [RMF] for DoD Information Technology [IT*]). In combination, these policies provide guidance on ICT SCRM for DoD personnel.

Although much of the available policy and guidance focuses on the development and production phases of the system development life cycle, most warfighting, intelligence, and business systems, products, and services spend the majority of their existence in the operations and sustainment phase. Risk management is essential during the design and manufacture phases of the system development life cycle because the decisions made have an impact throughout the life cycle, with implications for operations, routine services, maintenance, and planned upgrades or modifications. Decisions made during the acquisition phase can affect the system throughout its life cycle.

Updating Theme 3

The policies, standards, and strategies discussed in Theme 3, current in 2014 when the module was developed, are not comprehensive or well integrated, and do not offer clear guidance to personnel in every role, position, and organization about what to do in response to ICT supply chain risk. Theme 3 discusses the ICT SCRM responsibilities of certain roles and outlines actions for contracting, procurement, operations and sustainment, and disposal, but concrete activities and strategies are not well developed. The updated DoDI 5000.02 provides detailed guidance for program managers to mitigate cybersecurity risks across the acquisition life cycle, including supply chain security (USD[AT&L], 2015). Also, the controls listed in NIST SP 800-161 (Boyens et al., 2015) and the Cybersecurity Framework (NIST, 2017) provide the greater granularity and concreteness needed for action by personnel in government and the private sector.

DoD CIO continues to lead SCRM efforts for the DoD, the broader U.S. Government, and public-private partnerships (both domestic and international) with industry and academia. DoD CIO monitors and leads DoD implementation and improvement of DoDI 5200.44, contributed to the development of NIST SP 800-161, and partnered with NIST to rewrite the Committee on National Security Systems (CNSS) Directive 505, *Supply Chain Risk Management (SCRM)* (CNSS, 2012). DoD CIO, the Department of Homeland Security (DHS), NIST, and the General Services Administration (GSA) sponsor quarterly public-private Software and Supply Chain Assurance (SSCA) meetings to share SCRM best practices and lessons learned. DoD CIO and its FVEY partners (Australia, Canada, New Zealand, and the United Kingdom) sponsor a Supply Chain and Industrial Base Security Tiger Team that addresses SCRM issues from a FVEY and international military and coalition partner perspective. DoD CIO also works with non-profit and standards development organizations to raise awareness about SCRM and improve commercially acceptable global sourcing standards, which affect hardware assurance, software assurance, and assured services.

Status of Current ETA Programs

The authors engaged communities of interest to identify persons involved with ETA activities related to SCRM and supply chain security. Table 1 summarizes the outcomes of interviews conducted in the first quarter of 2017 with representatives of 28 organizations about their education, training, awareness, and guidance activities related to supply chain security. The organizations interviewed include the DoD, other federal agencies, private sector organizations, universities, and one community college. The authors also included

guidance activities from organizations that set standards, share information, and/or sell services or products that certify compliance with community best practices. The TSN Roundtable, the Diminishing Manufacturing Shortages and Material Shortages (DMSMS) Working Group, SAE, the National Defense Industry Association (NDIA), and the Aerospace Industries Association (AIA) are examples of such guidance groups.

Interviewees responded to personal invitations from one of the authors and/or an invitation distributed to members of various working groups/communities of practice. One of the authors conducted the interviews and summarized the key points. Some of the organizational activities described in Table 1 reflect a specific focus on supply chain risk, while others have a more general focus on software or cybersecurity.

Table 1. Organizations and Summary Comments

EDUCATION	
National Defense University (NDU), College of Information and Cyberspace	*Strategies for Assuring Cyber Supply Chain Security*, a graduate-level course, focuses on the systems development life cycle, the impact of counterfeits on cyber security, the DoD's trusted foundry, impacts on critical infrastructure, program protection planning and criticality analysis, the Defense Logistics Agency's role, microelectronics, and software assurance. Intended outcomes are the ability to assess organizational risk, develop a plan for increased awareness, and design a SCRM program based on current policies and best practices.
NDU, Eisenhower School of National Security and Resource Strategy	In a DoD acquisition practices- and policies-focused graduate course taught annually, one lesson includes threats to the supply chain (SC), relevant DoD perspectives and policies, and recent research. The intended outcome is increased awareness for better decision-making in the electronics industry. Student learning is assessed through final presentations on selected industries.
University of Detroit Mercy, Computer and Information Systems. Awareness of the importance of SC security is high in the auto industry.	*Secure Acquisition*, a graduate course, is offered annually and is based on best practices from NIST and the International Organization for Standardization (ISO) and research literature. Students are expected to implement a comprehensive, well-defined, organization-wide standards-based acquisition process; customize an appropriate set of acquisition activities for a given organization or project by life cycle phase; and organize, implement, and manage effective acquisition operations for a complex supply chain.
Worcester Polytechnic Institute, MA	*Supply Chain Risk Management* course developed for defense contractors focuses on the risks of counterfeit, tainted parts and products resulting from malware insertion into hardware, firmware, software, and circuit logic. Addresses threats to manufacturing and the integration of systems engineering practices into security engineering, critical infrastructure protection and information assurance, secure manufacturing practices, open software SC assurance, application security, and secure software development.

TRAINING AND AWARENESS	
AXELOS is a British joint venture between the UK government and Capita plc. It owns and nurtures global best practice frameworks and methodologies, including RESILIA, a cyber resilience best practice portfolio of certified training and awareness learning for all staff, for leadership engagement, and that includes a cyber maturity assessment tool.	Organizations and suppliers are being attacked, targeted, and breached, so response and recovery are now as important as detection and protection. An enterprise-wide response from the top must balance risks and opportunities as well as people, processes, and technology. Training is designed to fit personality differences and leverage multiple learning pathways depending on the risks and appetites of organizations and individuals with varied roles along the supply chain.
Black Duck Software helps companies identify and mitigate open source security risks across application portfolios throughout the life cycle and provides actionable, comprehensive lists of security, legal, and operational risks associated with components in use in a company's code base(s).	Increasing awareness about SC security begins with seeing what is in your code and understanding that software security is ephemeral and dependent on continuous monitoring for new vulnerabilities. To mitigate SC risk and leave an acceptable level of residual risk, options for vulnerable components are to rip and replace, patch, punt, and provide compensating controls.
Boeing, an aerospace company and leading manufacturer and exporter of commercial jetliners and defense, space, and security systems, supports airlines and U.S. and allied government customers in more than 150 countries. Boeing maintains a mature, risk-based security program for supply chain software that focuses on evidence and fact-based trust.	To reduce or eliminate security defects in vulnerable software, enterprise-class suppliers certify that their products were tested throughout the system development life cycle to demonstrate they are free of significant defects. Smaller, often third-party single-product suppliers provide evidence from mutually trusted sources that their software is free from significant, known security defects. Purchasing agents receive training on how to implement standards in various software contract types.
Defense Acquisition University (DAU), a corporate university in the DoD, offers courses to military and federal civilian staff and federal contractors. Two faculty experts and curriculum developers developed two supply chain courses that will be ready by the end of 2017. They offer faculty development, perform mission assistance across the DoD, and conduct SC security seminars.	Two online SC-focused courses, 3–4 hours each, offer guidance on how to address SC risks and provide links to guidebooks and polices for managing risk; they do not make recommendations for specific actions because circumstances vary widely. One is an overview of SCRM and SC logistics with a focus on counterfeits and trusted suppliers for understanding of SC risk and how to mitigate that risk from the point of program inception and throughout the life cycle—through assessments done early and often. The second is an introductory-level cybersecurity-focused course that looks at SCRM and counterfeiting of ICT components. Learners who pass the courses earn credits toward annual continuous learning requirements.
The Information Assurance Directorate (IAD) of the National Security Agency (NSA) is tasked with the information assurance mission and providing customers with confidence in cyberspace by identifying and correcting security vulnerabilities before adversaries exploit them without sacrificing the ability to use their systems effectively.	Two years ago, IAD developed a SCRM situational awareness module in information assurance that is now mandatory; a quiz was recently added. The organization also creates guidance for assessing risk in purchasing commercial solutions and a model for incorporating SCRM in capability packages. Guidance for mitigations is derived from security controls in NIST SP 800-53 Rev. 4 and DIACAP 8500.2. A forum exists for information sharing among government, industry, and academia.
Interos Solutions, a Washington, DC–based company, offers technical services, including vendor risk management; cyber and supply chain policy; and program risk management, critical infrastructure security, training, and awareness.	Increased attention to SC risk and cybersecurity, and changes in delivery methods are reported as shifts in traditional SCRM training. Cybersecurity is now integrated into larger enterprise risks. The NIST Cybersecurity Framework underscores that SC risk is part of the C suite's horizontal risk management. Awareness activities are increasingly computer platform-based and designed to push small segments to employees using tools and processes relevant to one's job and focused on specific threats and responses.

Office of the Director of National Intelligence, National Counterintelligence and Security Center	An awareness video is on YouTube. A 15-minute web-based SC fundamentals course is aimed at government employees and private sector partners. In the pipeline is a SCRM blueprint for contractors, with steps to develop a SCRM program and a companion on best practices. Standards for the intelligence community on criticality and threat assessment have been published; information sharing and vulnerability assessment courses are coming.
The Aerospace Corporation, a federally funded research and development center, provides technical guidance and support to government (intelligence community, military, and civil) and commercial customers to assure space mission success.	Classes are offered to customers about SCRM with a mission assurance perspective. They focus on the distillation and integration of government policies, requirements, and standards that are actionable and can be implemented by contractors. They also focus on SCRM recommended best practices to implement, and how to write requirements for contracts with prime contractors to ensure that the requirements will flow down to subcontractors. Additional classes will focus on how to secure the software development environment and the use of open source code for ASIC and FPGA development.
The University of Massachusetts (UMASS), a multi-campus public university that offers undergraduate, graduate, and professional degrees; collaborates with **itSMSolutions**, an online content solutions provider specializing in the delivery of video and instructor-led training solutions.	UMASS is improving its cybersecurity posture by creating training programs that focus on the knowledge, skills, and abilities to operationalize the best practice controls in the NIST Cybersecurity Framework across organizations and supply chains. Based on a NCSF controls factory methodology created by the university CISO, UMASS is partnering with itSMSolutions to offer online materials, video programs, online labs, mentoring services, and testing services designed to teach organizations how to protect their critical information assets and digital services.
U.S. Air Force Materiel Command	A CAC-enabled online course, “Introduction to Protection of Mission Critical Functions to Achieve TSN,” designed for acquisition and sustainment personnel, is ready for launch. It will provide an overview of requirements for mission assurance to support life cycle risk management. The course will increase awareness and knowledge of DoD efforts to field resilient systems through the TSN methodology; promote understanding of TSN terms, policies, and requirements and their importance to success in fielding resilient systems; and instill and maintain a continuing awareness of the ICT supply chain threats and vulnerabilities affecting mission-critical hardware and software.
U.S. Department of Energy (DoE), Office of the Chief Information Officer, SCRM Resource Center	Awareness, linked to cybersecurity awareness efforts, includes two learning modules—one for IT professionals and one for program managers; newsletters and posters; National Cybersecurity Awareness Month; internal postings; a quarterly speaker series; and a mini cross-agency working group of interest. In development is a mandatory program for authorizing officials of IT systems.
U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability in collaboration with the DHS Office of Infrastructure Protection	Focusing on the energy grid and suppliers, DoE collaborates with the Department of Homeland Security to research and develop SC security efforts that can be applied to the nation’s energy infrastructure. For awareness of cyber security and SC risks, webinars on relevant, innovative, and useful approaches to securing the supply chain are broadcast to manufacturers and electrical, oil, and natural gas organizations.
GUIDANCE TO ADVANCE KNOWLEDGE AND PRACTICE	
Electronic Components Industry Association, a membership organization that seeks to promote and improve the business environment for the authorized	SC security is a hot topic. Counterfeits are increasingly sophisticated, as evidenced by the increase in “generic” components to evade trademark infringement, mislabeling to appear to meet updated standards, remanufactured parts

sale of electronic components by manufacturers, their representatives, and distributors.	sold as new, and tainted programmable components. Cross-organizational forums set standards, and share information to keep members up to date.
Exostar, initially a joint venture of aerospace companies, seeks to remove redundancy in the SC process and increase security by protecting interactions with suppliers.	Leveraging identity, order, and access management processes, EXOSTAR's communication channels manage risk, increase cybersecurity, and reduce burden on suppliers and infrastructure. By assessing a suppliers' compliance with NIST 800-171 cybersecurity standards, system owners and prospective suppliers know the suppliers' cyber security posture and readiness.
Hemisphere Cyber Risk Management helps small businesses respond to cyber, legal, and insurance considerations to minimize their exposure to cyber and legal risk.	The focus is cyber risk management services that provide insight to improve cybersecurity investment strategies, and to make business- and cost-justified decisions on cyber risk, thus lowering total cost of ownership.
MITRE, a federally funded research and development center, promotes SC security with clients who are responding to government policies and directives. MITRE supports the DoD in reaching its awareness and compliance goals.	The DoD Risk Management Framework is taking hold at the grassroots level. Awareness has increased significantly, especially with communities with zero tolerance/no failure because of their missions. Intertwined cyber security and SC security require specific responses in implementation of system engineering practices.
NIST, U.S. Department of Commerce, Computer Security Division, conducts research and offers guidance. Cyber SC risk management work began in 2008 for federal departments and agencies with CNCI #11. Published first report on cyber SCRM in 2012 and official guidance for departments and agencies in 2015.	NIST activities range from formal briefings to training, as well as education, guidelines, and standards used by communities of interest and practice. SCRM is at the forefront of awareness in industry. The Cybersecurity Framework draft version 1.1 includes SCRM. Best practices case studies are posted on NIST's webpage, and industry best practices using anonymized lessons learned are in draft. Current research is on metrics, criticality analysis, predictive analytics modeling, and a quantitative approach to analyzing organizational interdependencies and associated risks.
Parasoft helps organizations deliver defect-free software efficiently.	A variety of training services support clients with continuous testing solutions for their organization's workflow to eliminate security risks through detection and prevention.
The Santa Fe Group specializes in thought leadership surrounding third-party risk management across the supply chain by providing expertise to all industry verticals, including critical infrastructure organizations, to mitigate third-party risk.	The membership-driven Shared Assessments Program identifies third-party risks and best practices in cybersecurity, IT, privacy, compliance, information security, and business resiliency controls. The program assists with assessing risk program maturity and provides "trust but verify" techniques and training, including the Certified Third Party Risk Professional program.
Software Engineering Institute, Carnegie Mellon University developed a software evaluation method that has evolved into a widely used multi-level capability and maturity model.	Continuing research on the Resilience Management Model and its higher level of risks in systems of systems, including hardware, software, and services in operational contexts; security engineering risk analysis; and external dependencies (supply chain) are integrated into courses at CMU and the Heinz executive program for CISOs.
Supply Chain Risk Management Consortium, an informal small business team of professionals with varied expertise; supports clients' development of resilient and secure supply chains.	The Consortium offers clients awareness and tools to increase the efficiency of their supply chains while reducing vulnerabilities such as exposure and counterfeits. The Consortium is considering developing a standards-based certification in supply chain risk, resilience, and security that employers will find valuable for their personnel.

The Open Group, a membership organization, developed the Open Trusted Technology Provider™ Standard–Mitigating Maliciously Tainted and Counterfeit Products (O-TTPS).	O-TTPS's best practice requirements for global SC security and COTS ICT product integrity help protect against maliciously tainted and counterfeit products throughout the COTS product life cycle. The O-TTPS Certification Program certifies IT providers (e.g., original equipment manufacturers [OEM], hardware and software component suppliers, value-add resellers and distributors) who conform to the standard. The Forum, a collaboration of government, academia, and the IT industry, develops and maintains the standard, also known as ISO/IEC 20243:2015.
U.S. Department of Homeland Security (DHS), DHS Science and Technology Directorate, Cyber Security Division	In response to the use of open source software and neglected hygiene of software, research is focused on improving, modernizing, and advancing the science of software assurance. Static analysis tools are being modernized to improve the visibility of software for consumers through ongoing collaboration with the NSA Center for Assured Software, NIST, and others.
Underwriters Laboratories standards, risk assessment services, and component certifications contribute to SC and cybersecurity.	Awareness of whether a component/product meets a minimum set of acceptable cybersecurity requirements is driven through publicly accessible cybersecurity certifications of specific manufacturers' products. Many different supply chain stakeholders, including end users, use these certificates. Procurement tools, press releases, white papers, webinars, direct marketing, government outreach, publications, presentations, and customer training are intended to help the full supply chain understand how to use the certifications to establish a baseline of cybersecurity hygiene.

These interviews revealed that some organizations, institutions, and communities increasingly understand supply chain risk and are actively responding with specific guidance and awareness efforts. The activities described in this informal survey focus on increasing awareness rather than changing behavior as an outcome of training. The guidance activities listed in Table 1 describe efforts made by membership and standards organizations and/or working groups that seek to advance the science, technology, and practice of supply chain security.

Supply Chain Security Throughout the Life Cycle

Although supply chain security is a focus of the acquisition phase of the system development life cycle, it is also critical during the operations and sustainment phase. As such, SCRM security must be considered not only during design and manufacturing, for example, but also during the operations and sustainment and disposal phases. Supply chain security cannot simply be evaluated only once in the system's life; it must be continually evaluated throughout the system's operation and sustainment and disposal. Once an acquisition program or system becomes operational, the suppliers, components, delivery processes, and business processes may change. These changes may alter or add supply chain risks. Most fielded systems, products, and services spend the majority of their existence—in some cases up to 80%—in the operations and sustainment phase of the system development life cycle. This means that ICT components are needed long after the authorized components are no longer manufactured. Repairing and replacing these components creates opportunities for counterfeit insertion, as well as other forms of tampering and exploitation. Supply chain security during the operations and sustainment phase of the life cycle calls for monitoring and periodically (or continuously) re-evaluating changes in risk, suppliers, operational environment, and use. Security efforts focused on replacement parts include purchasing parts from suppliers who understand supply chain security and providing information on any changes to the part, the part's operational environment, any vulnerabilities, and software patches to help manage supply chain risk.

The Trustworthy Supplier Framework

Background and Context

The Trustworthy Supplier Framework is a decision-support tool in development under the auspices of the Deputy Assistant Secretary of Defense for Systems Engineering (DASD[SE]) and the DoD Chief Information Officer (CIO) that emerged from the efforts of supply chain security communities of interest. Its purpose is to increase confidence in the security of products purchased from global commercial suppliers by designating qualified suppliers as "trustworthy." The framework could be used in a buyer's evaluation process, either as criterion for defining which suppliers are qualified or as part of the selection criteria. It may also be possible for a third party, either government or in industry, to act as an accreditation organization. Suppliers may find that having their businesses evaluated as being more "trustworthy" makes them more competitive in the DoD market for trusted products and components.

Like every purchaser, the DoD seeks to purchase trusted products and have confidence in the trustworthiness of its suppliers along its supply chain. Nevertheless, what constitutes a trustworthy supplier or product has not been well articulated. The Defense Microelectronics Activity (DMEA) defines a supplier as "trusted" based on the confidence in the supplier's "ability to secure national security systems by assessing the integrity of the people and processes used to design, generate, manufacture and distribute national security critical components" (DMEA, n.d.) such as microelectronics. In this context, a trusted supplier will:

- Provide an assured chain of custody for both classified and unclassified integrated circuits.
- Ensure that there will be no reasonable threats related to disruption in supply.
- Prevent intentional or unintentional modification of or tampering with the integrated circuits.
- Protect the integrated circuits from unauthorized attempts at reverse engineering, exposing functionality, or exposing vulnerabilities (DMEA, n.d.).

Using this definition, the Trustworthy Supplier Framework considers supplier and product trustworthiness to be based on confidence in the people and processes used to design, generate, manufacture, and distribute national security critical components and on evidence that a product is free of vulnerabilities (intentional and unintentional) that could compromise system or mission security.[7]

The evolving framework is a toolbox of vetted commercial standards and practices that suppliers can use to create trustworthy products. Instead of requiring commercial companies to invest in meeting government standards with uncertain financial return, the framework relies instead on familiar commercial standards and practices that will ease the financial burdens of compliance. The result—trusted products—will be comparable, even if the methods are not.

Current guidance speaks to what should be done about supply chain risk, but it does not provide specific steps, processes, or decision-making tools to mitigate risk. NIST SP

[7] This definition was adapted from DMEA's definition of "trusted" and NISTIR 7622.

800-161 guidance includes 236 controls that appear as a menu of options that requires refinement and expert judgment to select those of greatest relevance and importance. Toward that end, the Trustworthy Supplier Framework has the potential to enrich, spark, and supplement ETA efforts by prompting the acquisition workforce to look at their supply chains from a different perspective and use that perspective to enable better decision-making. The framework bridges the gap between relevant policies and standards and actionable controls. The Trustworthy Supplier Framework can also stimulate and enhance education, training, and guidance for the acquisition workforce by engaging learners in their own supply chain security assurance. By applying carefully selected standards, personnel can improve their processes, systems, and products to benefit everyone, thereby sharing responsibility for the increase in quality.

Framework Development

The origins of the Trustworthy Supplier Framework can be traced to discussions at DoD Trustworthy Supplier Working Group meetings and other gatherings of government, industry, and private sector personnel. In 2014, the working group identified a need for a toolbox for DoD acquisition personnel that would include industry standards for low-risk components, Defense Logistics Agency (DLA) supplier and product qualification for moderate-risk components, and DMEA Trusted Supplier requirements for critical components. The working group assigned a core team to define attributes of trustworthiness, develop a strawman framework of trustworthiness attributes, and align existing trustworthiness supply chain qualification approaches with those attributes.

Framework development began with a survey of government and industry standards and practices related to microelectronics SCRM. After a comprehensive review, the core team identified NIST SP 800-161 as the foundation for the Trustworthy Supplier Framework. The team then reviewed each control[8] in SP 800-161 to determine its relevance to determining a supplier's trustworthiness. SP 800-161 was written with a software focus, so the team interpreted control names and descriptions in the context of component acquisitions and hardware to align better with the framework's intent. Of the 236 controls listed in SP 800-161, 78 were found to be relevant.

The team then rewrote the names and descriptions of the relevant controls to fit a component acquisitions and hardware context. The team mapped the rewritten controls to common hardware vulnerabilities and then mapped the rewritten controls to relevant standards, regulations, and practices. The resulting matrix is cross-indexed and detailed, with controls mapping not only to certain standards and practices but also to specific sections of those standards and practices.

The Trustworthy Supplier Framework Approach

The Trustworthy Supplier Framework is a method for developing and applying system security engineering practices and controls to maintain the quality, safety, and security of DoD systems and missions. In the context of the framework, *quality* refers to systems that are available and work when needed, *safety* refers to the assurance that a system failure or error does not cost human lives, and *security* refers to system vulnerabilities and their susceptibility to compromise or exploitation. Each of these is a

[8] Controls are safeguards or countermeasures used to avoid, counteract, or minimize security risks.

system engineering function, and trustworthiness occurs at the intersection of the three. Ensuring quality, safety, and security, however, is a component-level concern as well as a system-level one. Quality, safety, and security concerns at the component level lead to system issues. The Trustworthy Supplier Framework approaches these functions at the component level (individual products and their suppliers) and offers controls to mitigate risks that would affect both the components and the systems they support.

The framework comprises a series of detailed spreadsheets—the rewritten controls and standards matrix—that function as a toolbox that both DoD personnel and commercial suppliers can use to define the needed level of product and supplier trustworthiness, and then select the appropriate controls to achieve that level. The framework also helps the DoD and commercial suppliers determine how best to implement the controls. Generally, controls state what should be done, but not how to do it. Without specific methods or desired outcomes, organizations can unintentionally select procedures that may be expensive, cumbersome, or less effective than desired. The rewritten controls use language familiar to DoD program personnel to facilitate better implementation. These rewritten controls can serve as a rubric that the DoD can use to assess trustworthiness in suppliers and products. For example, in the case in which one measure of trustworthiness might be compliance with framework controls, if company A complies with 28 controls and company B complies with 10, then the DoD can assume company A is more trustworthy.

The framework also helps improve the DoD's decision-making process for acquiring components beyond trustworthiness assessments. Currently, DoD program managers receive multiple sets of requirements for a single product and often do not have a path to satisfy multiple requirements with fewer actions. The rewritten controls in the framework provide a streamlined process, resulting in an integrated compliance path for multiple requirements. The DoD can also use the framework as a roadmap for determining how to engage with industry about current standards and develop new standards. The DoD has developed its own share of standards, but its efforts occurred without a great deal of industrial or commercial participation. Working with industry to develop and refine standards can be mutually beneficial.

Next Steps

Education, Training, and Awareness

Supply chain security begins with awareness of threats and vulnerabilities, and it is followed by informed decision-making that aligns with policies, available tools, and processes. ETA and guidance efforts need to be accompanied by adequate resourcing to implement the DoD's policies.

The education, awareness, and guidance activities discussed in the interviews are advancing supply chain security. As supply chain security tools, approaches, and processes are refined, training programs in supply chain security will become available for personnel in various roles. The Trustworthy Supplier Framework can become one of the drivers of this

training. Exercises designed to focus on supply chain security can identify needed training for acquisition, operations, and sustainment personnel.[9]

Evolving the Trustworthy Supplier Framework

The series of spreadsheets that comprise the Trustworthy Supplier Framework is just the first step. The next would be to turn the framework into a tool, perhaps available over a website. This tool could then be tested through pilot programs and studies that measure its effectiveness and cost benefits. Complying with government standards may come with certain high costs. In many cases it would be easier and less expensive for commercial companies to use their own standards and practices or adopt other industry standards. Measuring the cost benefits of doing so would validate the framework and promote its adoption.

The framework can also support the evaluation of the effectiveness of different control implementations, which might extend into a means of evaluating and qualifying or certifying suppliers as trustworthy.

References

40 U.S.C. § 11101, Definitions.

Boyens, J., Paulsen, C., Bartol, N., Moorthy, R., & Shankles, S. (2012, October). *Notional supply chain risk management practices for federal information systems* (National Institute for Standards and Technology [NIST] Interagency Report 7622).

Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N. (2015, April). *Supply chain risk management practices for federal information systems and organizations* (NIST Special Publication [SP] 800-161).

Committee on National Security Systems (CNSS). (2012, March 7). *Supply chain risk management (SCRM)* (CNSS Directive 505).

Defense Microelectronics Activity (DMEA). (n.d.). Trusted accreditation. Retrieved from http://www.dmea.osd.mil/trustedic.html

Defense Science Board. (2017, February). *Report of the Defense Science Board Task Force on cyber supply chain.*

Department of Defense Chief Information Officer (DoD CIO). (2014a, March 14). *Cybersecurity* (DoD Instruction [DoDI] 8500.01).

DoD CIO. (2014b, March 12). *Risk management framework (RMF) for DoD information technology (IT)* (DoDI 8510.01).

DoD CIO & Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L]). (2012, November 5). *Protection of mission critical functions to achieve trusted systems and networks (TSN)* (DoDI 5200.44).

[9] The Defense Science Board Task Force on Cyber Supply Chain released a report in February 2017 that recommends that military service chiefs conduct at least one Cyber Awakening exercise per year and use the results to drive and update training. Cyber Awakening exercises identify vulnerabilities and monitoring activities and promote vulnerability-related information sharing (Defense Science Board, 2017).

DOD Dictionary of Military and Associated Terms. (2017, February). Retrieved from the Joint Electronic Library: http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf

McDaniel, E., Barth, T., & Albert, M. (2014). *Managing information communication technology global supply chain risk—Awareness module*. Alexandria, VA: Institute for Defense Analyses.

National Institute for Standards and Technology (NIST). (2010, February). *Guide for applying the risk management framework to federal information systems: A security life cycle approach* (NIST SP 800-37 Revision 1; updated June 5, 2014).

NIST. (2013, April). *Security and privacy controls for federal information systems* (NIST SP 800-53 Revision 4).

NIST. (2017, January 10). *Framework for improving critical infrastructure cybersecurity*. Draft Version 1.1.

Ross, R., McEvilley, M., & Oren, J. C. (2016, November). *Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems* (NIST SP 800-160).

Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L]). (2015, January 7). *Operation of the defense acquisition system* (DoDI 5000.02). Washington, DC: Author.

Under Secretary of Defense for Intelligence (USD[I]) & USD(AT&L). (2015, May 28). *Critical program information (CPI) protection within research, development, test, and evaluation (RDT&E)* (DoDI 5200.39).

Acquisition Research Program
Graduate School of Business & Public Policy
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net