We Cannot Blindly Reap the Benefits of a Globalized ICT Supply Chain!

Don Davidson, Office of the DoD Chief Information Officer
Stephanie Shankles, Booz Allen Hamilton

Abstract. Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM) seeks to manage and mitigate cyber and supply chain risk throughout an acquisition and sustainment lifecycle for an element or a system. It is a multi-disciplinary challenge that requires contributions and collaboration among many disciplines. Key areas include systems engineering, system security engineering, information security, software development, application security, supply chain and logistics planning and management, IT resiliency, and risk management. While many areas are making great strides in developing and implementing best practices and tools to combat their individual cyber challenges, it is imperative for successful enterprise risk management to view the challenge holistically and align common best practices and initiatives, some from/for the public sector and some from/for the private sector.

Introduction

A holistic view of supply chain risk management is one of the 12 key areas in the United States Comprehensive National Cyber Security Initiative (CNCI). CNCI-SCRM is a Federal Government wide multi-pronged approach for managing risk while operating in a global supply chain. Managing this risk requires a greater awareness of the threats, vulnerabilities, and consequences associated with acquisition decisions; the development and employment of tools and resources to technically and operationally mitigate risk across the lifecycle of systems, products and/or elements (from design through retirement); the development of new acquisition policies and practices that reflect the complex global marketplace; and partnership with industry to develop and adopt supply chain and risk management standards and best practices.

"Software and hardware are at risk of being tampered with even before they are linked together in an operational system. Rogue code, including so-called logic bombs, which cause sudden malfunctions, can be inserted into software as it is being developed. As for hardware, remotely operated "kill switches" and hidden "backdoors" can be written into the computer chips used by the military, allowing outside actors to manipulate the systems from afar. The risk of compromise in the manufacturing process is very real and is perhaps the least understood cyberthreat. Tampering is almost impossible to detect and even harder to eradicate."
(DEPSECDEF Lynn in FOREIGN AFAIRS in Sep 2010.)

Globalization has brought a unique set of SCRM challenges and threats to the U.S. Government and industry, especially with our ever-increasing reliance on ICT products and services to meet mission and business needs and the interconnected nature of our IT systems. Threats to the ICT systems are varied, complex and demonstrate a wide array of motivations for attack. They range from counterfeit items made for a quick profit, intentional threats such as malicious code or hardware Trojans, to poor software development practices that create software vulnerabilities or hardware quality issues. These are all the more dangerous because ICT is found everywhere in our environment, from our home entertainment systems, mobile devices that hold/move our personal information, to our infrastructure's financial and energy sectors, and even to national security systems and weapons systems.

Challenges With Globalization

Globally, USG represents a relatively minor share of the ICT product and service market for the industry and alone does not command the market power to drive commercial suppliers to substantially change their SCRM practices. However, USG is an important stakeholder in the process because of their role in national and global security and the variety of valuable lessons learned and best practices they can provide because they are such a diverse organization. The ICT SCRM challenge is not limited to USG, it impacts every government and commercial organization that acquires and uses ICT products and services. Furthermore, many of the suppliers of ICT products and services also find themselves acquiring ICT products and services to integrate into their own solutions and therefore have a common interest in facing the ICT SCRM challenge.

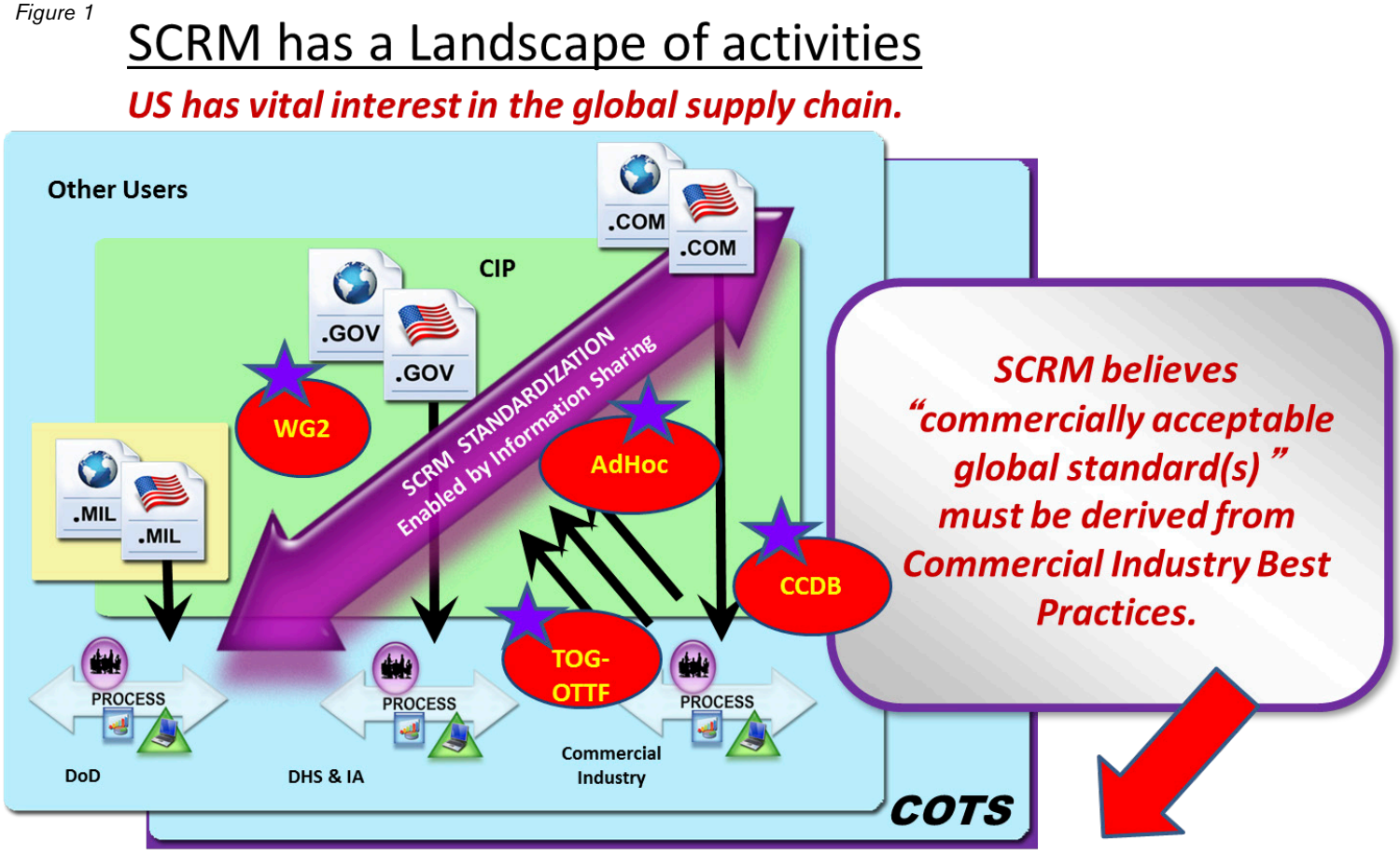
Federal acquirers and commercial acquirers and suppliers are all increasingly interconnected and interdependent in a global supply chain, both physically and digitally. We, in USG are not as independent as we used to be; we have fewer unique capabilities, systems and components. We all leverage an increasing number of COTS products, including hardware, software and services. However, our mission remains unique, and in the interest of national security and warfighter support, mission critical acquisitions need to be evaluated in terms of product integrity, mission assurance and SCRM best practices.

In this budget-conscious environment, there is no way to return to a supplier base of "all-American" companies for the U.S. Government's ICT acquisitions, nor can we have complete confidence that even American made products are free of supply chain vulnerabilities. Knowing what challenges we face by applying SCRM practices and guidance to our acquisition processes will help us tackle our next big challenge, which is to build weapons systems and information networks that are resilient against the most sophisticated cyber adversaries using mostly commercial and potentially untrustworthy products and services. This is both a sourcing and a systems engineering challenge.

Addressing the SCRM Challenge

GAO recently published GAO Report-12-361 Code 311064, "IT Supply Chain: National Security-related Agencies Need to Better Address Risks." They endorsed DoD SCRM strategy and implementation and recommended it as a model to others. The Committee on National Security Systems (CNSS) recently published CNSS Directive 505 on Supply Chain Risk Management. GAO said DoD's efforts to implement SCRM can be a learning tool for others in the Federal government. DoD is currently imple-

Figure 1



menting a strategy for achieving trusted systems and networks to address this challenge which has four key tenets: prioritizing resources based on mission dependence; comprehensive program protection planning; enhanced vulnerability detection, and industry partnership. This trusted systems and networks strategy is being implemented through existing Program Protection and Information Assurance processes through the recently published DoD policy DoDI 5200.44 – "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks." It integrates existing disciplines of SCRM, system security engineering, counterintelligence, hardware and software assurance among others, to reduce the likelihood that warfighting capabilities will be impaired due to vulnerabilities in system design or sabotage of a system's critical functions and components. The policy builds on best practices, lessons learned, and evolving thinking from more than four years of piloting and incremental implementation within the Department by requiring specific program protection and SCRM activities to protect the most critical DoD systems. We continue to work across the Department and with our fellow interagency partners, our suppliers, and our system integrators to implement a risk management strategy into other government organizations (and their suppliers) and the country's wider Critical Infrastructure Protection initiatives.

As we develop better visibility into the global supply chain and improved trust in the products we consume or use we will be able to develop more resilient system designs, which will move us from a "risk response posture" to a more proactive, "risk prevention, risk mitigation, or even risk endurance posture."

In Figure 1, the large purple arrow highlights information sharing as the key to harmonizing SCRM efforts currently being addressed by different stakeholders, such as the civil government agencies, defense agencies and private industry. A number of active joint efforts and information sharing forums exist, as noted by the red circled items. The Open Group's Open Trusted Technology Forum is a collaborative effort between government and industry and is currently developing a framework of SCRM best practices for use by industry. The SCRM Lifecycle Processes and Standards Working Group meets almost monthly and is a DHS-DOD CNCI-11 (SCRM) effort co-chaired by DoD and NIST representatives and serves as an interagency sharing and collaboration venue. The Cyber Security 1 (CS1) ICT SCRM Ad Hoc group is comprised of civil and defense/government representatives and industry stakeholders. The primary focus is SCRM input and development of international standards, as CS1 supports the International Organization for Standardization (ISO). Finally, the Common Criteria Development Board (CCDB) is an ISO based effort supported by industry and government participation and is actively incorporating SCRM into the CC certifications for global use.

Working With Industry

Product development (from design through manufacturing, integration, and delivery) typically involves an array of developers and suppliers around the world, many of whom the end user

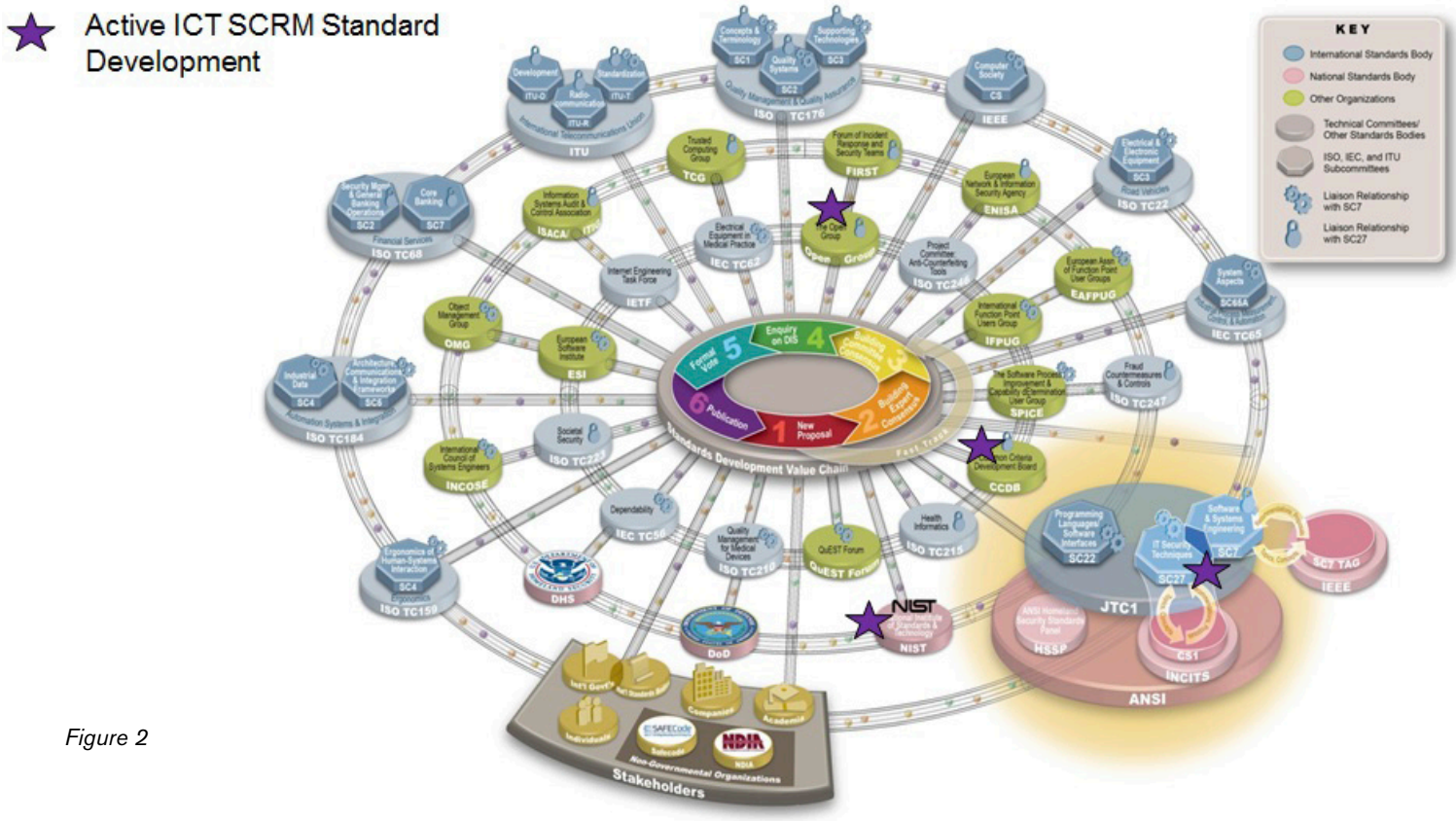


Figure 2

does not know. As a consequence of our global supply chain, adversaries have more opportunities to corrupt technologies before we take ownership and introduce malicious, tainted or counterfeit code or hardware into the supply chain. And even outside of the maliciously altered products, these incredibly complex, commercial products may at times have vulnerabilities unintentionally left in as they leave the product line. These vulnerabilities may be tolerable in cell phones and video games, but could prove catastrophic in a fighter jet or classified network as such vulnerabilities may make it easier for adversaries to use remote access attacks to otherwise gain access to the USG's systems and networks.

DoD has been working internally to enhance its acquisition, engineering, and sustainment processes, while simultaneously working externally with commercial industry to advocate improved product development standards to reduce vulnerabilities in commercial products related to global sourcing. The study of ICT SCRM standards landscape was completed in January 2010 in the form of a document and a key graphic provided in Figure 2.

The graphic and the corresponding Standards Landscape document are based on the portfolio of two international committees under the auspices of ISO/IEC JTC1 – SC 27 that focuses on IT Security Techniques and SC7 that focuses on System and Software Engineering. The graphic is color-coded as follows:

- Blue indicates Standards Development Organization (SDO) groups associated with ISO, IEC, or ITU
- Green indicates other SDOs
- Pink indicates US-based organizations including the Technical Advisory Groups for SC7 (SC7 TAG) and SC27 (CS1), their parent organizations (IEEE and ANSI), as well as US government agencies engaged in the development of ICT SCRM standards (NIST, DoD, DHS)
- Purple stars indicate specific SDOs currently engaging in the development of ICT SCRM content, both nationally and internationally, including SC27, SC7, The Open Group, CCDB, and NIST. Note these same starred areas are where DoD chose to engage with their information sharing activities.

The standards landscape identified a variety of groups that are engaging in the collection/development of ICT SCRM or related content and helped prioritize DOD engagement in these groups, as well as the areas of focus. Based on the outputs of landscape DOD has engaged with multiple stakeholders and continues identifying other potential stakeholder groups to facili-

tate information sharing.

The standards landscape review led DOD standardization activities towards specific SDOs to focus on standardization for ICT SCRM. The standards landscape also recommended relevant standards efforts within SC27 and SC7 for participation, influence, and monitoring based on the overall DOD engagement framework. DoD is actively working to coordinate external standards efforts with the DoD IT Standards Registry.

Based on the landscape DOD focused its standardization on CS1 and worked with CS1 to establish and Chair CS1 ICT SCRM Ad Hoc that is a joint group with SC7 TAG. The Ad Hoc is a non-voting group that has the authority to review SC27 and SC7 standards distributed to US National Bodies (CS1 and SC7 TAG) for review and comment, works to achieve consensus on a single position, and then recommends positions for vote and approval by CS1 or SC7 TAG as US positions to be submitted to SC27 or SC7.

As the efforts progressed, other areas of focus were identified including The Open Group, North American Security Products Organization, Information Security Forum, Object Management Group, Common Criteria / ISO15408 and SAE(G19), etc. Trusted Mission Systems and Networks continues identifying additional SDOs for potential collaboration through the current participation in various SDOs. These efforts were identified based on the inputs received from individual participants in the standardization processes, as well as to ensure that CS1/SCRM AdHoc WG references relevant documents that are either already in the standards domain or in the process of being developed.

Conclusion

The SCRM community/stakeholders know that change will not happen overnight and the implementation of this kind of comprehensive acquisition risk management for all of our systems and networks will take the investment of resources, time and funding. Therefore a key element of the SCRM strategy is to prioritize capabilities and their enabling systems and subcomponents; identify our critical systems and plan for and build in more trust, using a risk based approach.

In DoD we continually seek to improve our capabilities and cyber posture; improving our capability to detect cyber problems in our day-to-day operations, but that still puts us in a "risk response posture"; we need to better understand the components within our systems that enable our mission critical capabilities (we call this criticality analysis); where do we source the critical hardware, software, and services for those systems (especially national security systems and critical infrastructure), and how should we better design and manage our systems to minimize vulnerabilities and assure critical functions, even when a system is under attack. Understanding and managing the risk associated with those systems and their components, will make us and our systems more resilient.

Recently, there has been a lot of news on microelectronic counterfeits, malicious or poor quality software and data breaches. All of these topics have roots in our global supply chain. Do not misunderstand our intent, this is not about becoming isolationists—DoD embraces globalization and will continue to reap cost and schedule benefits from it every day—but we do need to be more sensitive to the system and/or information security and product and/or data integrity implications, to our systems and ultimately our capabilities, when outsourcing key components and capabilities. We need to better "see" into some legs of the supply chain, especially where critical components are involved.

DoD is doing well in our strategy and implementation on SCRM, however we are developing capability through a "crawl-walk-run" process which has dependencies on potentially diminishing resources and external support, like private sector cooperation.

For additional information or to get involved in SCRM efforts, contacts are listed in Table 1.

Stakeholder Audience	Ongoing Effort	Points Of Contact
Department of Defense	Trusted Systems and Networks Round Table	Joe Wassel – joe.wassel@osd.mil Melinda Reed – melinda.reed@osd.mil
Interagency Coordination	CNCI SCRM Working Group 2	Don Davidson – don.davidson@osd.mi Jon Boyens – jon.boyens@nist.gov
Critical Infrastructure Protection	DHS SCRM DHS Software Assurance	Joe Jarzombek – joe.jarzombek@hq.dhs.gov
ISO Standards and Harmonization	CS1 ICT SCRM Ad hoc	Don Davidson – don.davidson@osd.mil Nadya Bartol – nadya.bartol@utc.org

Table 1: SCRM Effort Contacts

ABOUT THE AUTHORS

Don Davidson is assigned to Trusted Mission Systems and Networks in the Office of the Department of Defense Chief Information Officer (DoD CIO), as Chief, Outreach, Science, and Standards (CNCI-SCRM). He has 37 years of federal service to include 11 years active duty, as well as civilian assignments in Army Research Laboratory, Army Materiel Command, Army Secretariat, US Joint Forces Command, OUSD-Acquisition, Technology & Logistics (AT&L), and DoD CIO.

E-mail: Don.Davidson@osd.mil

Stephanie Shankles of Booz Allen Hamilton, is a subject matter expert in software assurance and ICT supply chain risk management. She supports projects ranging from IT policy development to IT security training to helping clients integrate security processes throughout their project lifecycle. She is currently supporting industry efforts to develop and implement ICT supply chain risk management guidelines and standards. She has spoken at multiple industry events on software assurance implementation, benchmarking and measurement.

E-mail: shankles_stephanie@bah.com