

STATEMENT BY

MITCHELL KOMAROFF

**OFFICE OF THE DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
TRUSTED MISSION SYSTEMS & NETWORKS**

**BEFORE THE
HOUSE ENERGY & COMMERCE COMMITTEE
SUBCOMMITTEE ON OVERSIGHT & INVESTIGATIONS**

ON

IT SUPPLY CHAIN: REVIEW OF GOVERNMENT AND INDUSTRY EFFORTS

March 27, 2012

**NOT FOR PUBLICATION UNTIL RELEASED BY THE SUBCOMMITTEE ON
OVERSIGHT & INVESTIGATIONS, COMMITTEE ON ENERGY & COMMERCE**

Summary

Once dominated by domestic manufacturing, today's information communications technology (ICT) manufacturing is global, and increasingly performed outside of the United States.

Although the globalization of the ICT sector has accelerated the pace of technological innovation, it has also raised national security concerns that ICT hardware and software performing critical functions within its weapons and networks may contain malicious code.

In response to the forgoing globalization and supply chain risks, DoD is in the process of institutionalizing a Trusted Systems and Networks Strategy, which contains four elements: 1) Prioritize scarce resources based on mission dependence; 2) Plan for comprehensive program protection; 3) Detect and respond to vulnerabilities in programmable logic elements; and 4) Partner with industry.

The Department has undertaken an incremental approach to supply chain risk management through a series of acquisition pilot programs beginning in FY09 and FY10. DoD is now institutionalizing lessons learned during the piloting phase into permanent policy and practice. Part of DoD's strategy moving forward is to actively engage industry by participating in key standards development organizations (SDO) and reaching out at major community events, soliciting and collecting inter-agency and industry feedback, and working to develop and incorporate industry feedback into work products at the national and international levels. DoD also works with other Departments and Agencies to share lessons learned and drive best practices from piloting into USG-wide policy. Most recently, DoD and DHS worked with the Committee on National Security Systems (CNSS) to develop CNSS Directive 505 - Supply

Chain Risk Management, which serves as the supply chain policy that applies to all National Security Systems within the federal government.

Introduction

Good Morning Mr. Chairman and distinguished members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee on the Department of Defense's efforts pertaining to supply chain risk management. I am Mitchell Komaroff, and I am the Director of Trusted Mission Systems & Networks within the Office of the DoD Chief Information Officer (CIO). The Government Accountability Office (GAO) report being discussed today examines the challenge posed by insufficient security in the information technology (IT) supply chain that has the potential to lead to the exploitation of Federal networks and information. The Department of Defense (DoD) takes this challenge seriously, and is undertaking a number of steps to ensure that risks relating to the DoD's global supply chain for IT do not disrupt our ability to defend the nation. I would like to give you an overview of the challenge as it pertains to the Department and highlight our current strategy.

A. Globalization Challenge

The Department relies heavily on customized and commercial off-the-shelf (COTS) computers, communications equipment, integrated circuits (ICs), application software, and other information communications technology (ICT) to stay on the cutting edge of technology development and fulfill mission-critical operations. With increasing frequency, the Department and its commercial supplier base rely on foreign companies to produce the most advanced technology solutions. Once dominated by domestic manufacturing, globalization has caused today's ICT

manufacturing to be largely conducted outside of the United States. Globalization has led to rapid technology innovation, from which the DoD benefits greatly.

Although the globalization of the ICT sector has accelerated the pace of technological innovation, it has also raised national security concerns. Mission-critical functionality of the Department's systems and networks extensively leverages commercial, globally interconnected, and globally sourced ICT. A highly capable malicious actor can employ a full spectrum of offensive and exploitation capabilities by using a deep knowledge of latent vulnerabilities and supply chain attacks to create new vulnerabilities. As a result of this diverse global supply chain, adversaries have more opportunities to corrupt technologies, introduce malicious code into the supply chain, and otherwise gain access to the Department's military systems and networks. There is no way to return to a supplier base of "all-American" companies for the Department's ICT. Although some programs use secured facilities and cleared personnel to protect classified information when developing technology for sensitive government use, this approach is neither ideal nor financially feasible on a large scale.

B. DoD Strategy and Implementation

Background

For years, the Department has known of the risk that ICT hardware and software performing critical functions within its weapons and networks may contain malicious code and has been working to address this risk. By 2003, DoD could no longer afford to internally produce leading edge application specific integrated circuits (ASICs), and so established the Trusted Foundry program to ensure trusted, leading edge military unique chips could be acquired from commercial industry. In the 2004-2006 timeframe, DoD CIO and the Under Secretary of

Defense for Acquisition, Technology and Logistics (USD(AT&L)) considered similar issues associated with software within their Software Assurance Tiger Team effort. This effort elevated the software/hardware issues to the systems-level, and formulated a full lifecycle strategy involving system prioritization, identification and protection of critical system functions and ICT components, use of all source intelligence to understand supply chain risk, enhanced test and evaluation for vulnerability detection, and industry engagement. These strategy elements and the key partnership between information assurance and acquisition continue to animate DoD policy and implementation as described below.

Trusted Systems and Networks Strategy

In response to the forgoing globalization and 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:

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).

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. Our 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. The critical components so identified become the focus of protection activities, including use of all source threat analysis to identify supply chain risk, and enhanced test and evaluation.

3. **Detect and respond to vulnerabilities in programmable logic elements** – Invest in enhanced vulnerability detection research and development, and transition such analytical capabilities to support acquisition.

4. **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.

Incremental Implementation

Supply Chain Risk Management (SCRM) represents a change in the acquisition process. It requires new institutional relationships between acquisition and the intelligence community, and

application of operations security to processes that have historically sought to be transparent. Beginning with the Comprehensive National Cyber Security Initiative (CNCSI) Initiative 11 in 2008, co-led by DoD and the Department of Homeland Security (DHS), the DoD strategy has been incremental implementation of the new processes and practices through pilots. DoD Directive Type Memorandum (DTM) 08-048, February 19, 2009, “Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems” provided the framework for DoD implementation of SCRM.

In DTM 08-048 (reissued March 25, 2010, 09-016), DoD Deputy Secretary Lynn directed incremental implementation of SCRM as outlined in the above strategy beginning with pilots in FY09/10 and requiring full operational capability by FY16 for all NSS. The DTM also established the mission at the Defense Intelligence Agency (DIA) to provide supply chain threat analyses to DoD acquisition programs, and directed vulnerability assessments to meet the requirements of FY09 NDAA Section 254.

The key objectives in FY09/10 were:

- 1) Establishing institutional relationships between Military Department (MILDEP) acquisition programs (through then “SCRM Centers of Excellence” now “SCRM Focal Points”) and the new DIA Threat Analysis Center (TAC) threat assessment capability;
- 2) Developing, evaluating, and documenting SCRM best practices in the DoD SCRM Key Practices Guide; and
- 3) Performing FY09 NDAA Section 254 Congressional direction.

During this period, DoD performed “Center of Excellence” pilots and vulnerability assessments under FY09 NDAA Section 254, during which acquisition programs leveraged DIA TAC analysis, and assessed practices within the DoD SCRM Key Practices Guide. These activities validated DoD strategies, confirmed that SCRM was necessary to manage risk being assumed by DoD programs, and exercised new DIA TAC intelligence capabilities. FY09/10 pilots were documented in the Section 254 “Trusted Defense Systems” Report to Congress in December of 2009, and “CNCI DoD Supply Chain Risk Management (SCRM) Pilot Program Report” in April of 2011. During this period, based upon lessons learned, DoD engaged with its oversight committees to seek clarification to use new intelligence capabilities within its procurement processes, leading to FY11 NDAA Section 806, “Requirements for Information Relating to Supply Chain Risk.”

DoD is currently institutionalizing lessons learned during the piloting phase into permanent policy and practice.

- 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 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.
- Lastly, we are working to fully implement FY11 NDAA Section 806, which clarifies DoD authority to use intelligence within its procurement processes. The statute sets forth procedures that enable DoD under specified circumstances to exclude a particular source who presents an unacceptable level of supply chain risk, and withhold certain information regarding the basis of that decision. DoD is working through a series of tabletop exercises and pilots to determine the best way to integrate the authority into its processes.

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.

C. Partnership with Industry

DoD engages in a robust collaboration with industry to collect, analyze and share SCRM best practices and to better understand the level of risk the USG accepts when procuring ICT from commercial suppliers and integrators. DoD's strategy is to actively engage industry by participating in key standards development organizations (SDO) and reaching out at major community events, soliciting and collecting inter-agency and industry feedback, and working to develop and incorporate industry feedback into work products at the national and international levels. Additionally, DoD collaborates along with the National Institute for Standards and Technology (NIST) in the DHS-led Software Assurance (SwA) Program. The SwA Program hosts quarterly Forums & Working Groups to bring together members of government, industry, and academia with vested interests in software assurance to discuss and promote integrity, security, and reliability in software, in the supply chain.

One of the key standardization and outreach goals is to facilitate development and adoption of commercial global sourcing standards, which will enable DoD and other USG acquirers of ICT products and services to better communicate in ICT requirements, and to establish industry practices for validating those requirements have been satisfied. To achieve this goal, DoD is engaged in several key national and international standardization efforts, including the

International Organization for Standardization (ISO) and other key SDOs. In addition, the Department partners with over 20 government and industry organizations as well as the Information Security Forum (ISF), a global non-profit with 300 corporation members, towards the development of commercially-reasonable standards for global sourcing.

DoD is also engaged in The Open Group's "Trusted Technology Forum" (OTTF). The OTTF strives to provide a collaborative, open environment for technology companies, customers, government, and supplier organizations to create and promote guidelines for manufacturing, sourcing, and integrating trusted, secure technologies, shape global procurement strategies and best practices to help reduce threats and vulnerabilities in the global supply chain. OTTF recently released a "snapshot" of their "trusted technology provider framework" (TTPF) which documents best practices against counterfeits and tainted products. DoD is working with OTTF to foster standards harmonization with the existing "mutual recognition" Common Criteria for product evaluations and other related ISO / international standards.

These are just a few of the venues where DoD collaborates with a variety of other government, industry, and public/private activities to solve the ICT SCRM challenge. In the next 3 years, DoD strives to move these various efforts forward with the goal of having a family of related ICT SCRM standards available for USG and industry to use for establishing mature relationships with ICT service and product providers. The ultimate goal of the standardization efforts is to help raise the bar of best practice globally to help create a more transparent environment for acquirers of ICT services and products.

D. Way Ahead

DoD continues to march towards full scale implementation of DoD's SCRM Program while participating in CNCI and partnering with the Committee for National Security Systems (CNSS) and other agencies to advance SCRM efforts across mission critical USG systems and networks. Within DoD, a key objective for 2012 is developing an integrated set of information assurance and acquisition policies to reflect SCRM concepts. DoD CIO and USD(AT&L) will continue to support the Military Services and Defense Agencies as they build out their capabilities and will provide guidance and support to programs on how to identify and manage risk they may have already accepted. Training, education, and awareness efforts will be an important part of these efforts going forward.

Since its efforts in CNCI Initiative 11, DoD has collaborated with the Interagency regarding proposed policies, processes and SCRM best practices. The DoD SCRM Key Practices were shared with DHS and NIST at an early point, and have been made available to the larger community as the NIST Interagency Report 7622, "Supply Chain Risk Management." In the area of Policy, DoD Directive Type Memorandum 09-016, "Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems" and its draft Instruction 5200.MM, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks" have been shared with the Interagency, and through the Committee on National Security systems (CNSS) Directive 505, "Supply Chain Risk Management" has been made binding on all USG National Security systems.

CNSS Directive 505, “Supply Chain Risk Management” adopts concepts, lessons learned and strategy elements from the DoD’s SCRM strategy and issuances, including elements of the incremental approach to implementing SCRM. Within the first year of 505’s issuance, agencies are to develop an initial SCRM capability, and within six years of the issuance’s publication, agencies are to have developed a full-scale SCRM capability to protect their NSS. This model has been successful in the DoD, and through lessons learned has set the stage for a successful implementation by interagency.

Conclusion

Mitigating risks to the Department’s missions from the global supply chain for ICT is critical to our national security. The efforts that I have outlined today detail what the Department has done and is planning to continue to do to ensure effective supply chain risk management. I want to thank you for your interest in our efforts and I am happy to answer any questions you may have.