SUPPLIER-SUPPLY CHAIN RISK MANAGEMENT (S-SCRM)

Dr. Serena Chan

The Problem

The growing trend of globalization and outsourcing provides opportunities for adversaries to penetrate the Government's supply chain of information and communications systems. Their purposes might be to obtain knowledge, gain access, insert malicious code, or corrupt information or components bound for mission-critical systems and networks. Supply chain risk is an increasing concern as globalization produces more complex supply chains, and outsourcing creates greater dependency on external suppliers instead of developing products in controlled or trusted environments.

> **The complex, transitory, and global nature of the commercial ICT marketplace makes it challenging to assure that articles of supply and the suppliers can be trusted to do only that which is expected or specified...**

Supply chain risks must be evaluated early and continually throughout the acquisition life cycle in order to effectively develop and implement defensive countermeasures and mitigations. Risks can be introduced at any point in the supply chain and may be passed along downstream to intermediate product and service users or end-users. IDA is supporting its sponsor in developing supply chain risk management (SCRM) capabilities that are responsive to the increasing dependencies on information and communications technology (ICT) that enable trusted mission systems and networks.

National Security Presidential Directive 54/Homeland Security Presidential Directive 23 created the Comprehensive National Cybersecurity Initiative (CNCI) to improve how the Federal Government protects sensitive information on agency networks from cyber threats. CNCI includes 12 efforts that either formalize existing cybersecurity processes or introduce new policies and business practices to better protect computer networks and systems. CNCI Initiative 11 called for DoD and DHS to lead an interagency effort on SCRM.

DoD increasingly relies on ICT components and services to support its critical information and weapons systems. The complex, transitory, and global nature of the commercial ICT marketplace makes it challenging to assure that articles of supply and the suppliers can be trusted to do only that which is expected or specified and to do so reliably and dependably. To help address this challenge, DoD established a SCRM Pilot Program.

The SCRM Pilot Program is intended to improve DoD's understanding of what practices work effectively; what gaps exist in policy and guidance; how the current or proposed practices, processes and procedures for discovering, using, and managing risk information perform; what general impediments to implementing robust supply chain risk management for the acquisition of ICT exist; and what the anticipated cost, schedule, and performance impacts may be. The pilot activities are also intended to validate the timeliness and actionability of all-source intelligence available to acquisition professionals.

IDA has developed and continues to refine the Key Practices and Implementation Guide for the DoD SCRM Pilot Program.[1] This document provides insights and methods to mitigate risks that arise from the suppliers in a DoD acquisition program. It includes examples of practices expected to mitigate identifiable vulnerabilities and associated threats. Each practice has the potential to impact procurement or an acquisition's cost, schedule, or performance.

IDA also assisted in standing up the Threat Assessment Center (TAC) in the Defense Intelligence Agency and continues to provide analytic support and develop training. Additionally, IDA conducted vulnerability assessments on selected covered acquisition programs, studied techniques for verifying trust in Integrated Circuits (IC), and validated DoD's Strategy for Systems Assurance and Trustworthiness. IDA continues to support additional vulnerability assessments, criticality integration, and prioritization efforts. Related outreach activities have included IDA presentations at the 15th Republic of Korea – United States (ROK-US) Defense Analysis Seminar, the 2010 Military Communications Conference (MILCOM), and the 2010 Institute of Electrical and Electronics Engineers (IEEE) International Conference on Technologies for Homeland Security.[2]

IDA is helping DoD discover, define, learn, and establish capabilities related to supplier and supply chain risk management (S-SCRM) of ICT. Integral to this has been the development of an S-SCRM enterprise framework that brings together intelligence mitigations, technical mitigations, and business mitigations into a trade space to reach a collective view and to review and adjudicate decisions to obtain a Risk Reduction-Return on Investment (RR-ROI), illustrated in Figure 1. *Intelligence mitigations* refer to the ability to apply knowledge to manipulate one's environment or situation. *Technical mitigations* refer to measures to alleviate the consequences of a realized flaw or failure potential in an item of supply. *Business mitigations* are the process capabilities that use and apply knowledge, know-how, and tools to conceive, design, develop, produce, deliver, and sustain

[1] US Department of Defense, *Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11 Supply Chain Risk Management Pilot Program*, February 25, 2010.

[2] [(a)] Greg Larsen and Forrest R. Frank, "Assuring Operational Readiness through Management of Supply Chain Risks," *15th Republic of Korea – United States (ROK-US) Defense Analysis Seminar*, Seoul, Republic of Korea, April 13-17, 2010. [(b)] "Cybersecurity Supplier-Supply Chain Risk Management," 2010 MILCOM Classified Technical Panel, *Military Communications Conference (MILCOM) 2010*, San Jose, CA, October 31 – November 3, 2010. [(c)] Serena Chan and Gregory N. Larsen, "A Framework for Supplier-Supply Chain Risk Management: Tradespace Factors to Achieve Risk Reduction – Return on Investment," *2010 IEEE International Conference on Technologies for Homeland Security*, Waltham, MA, November 8-10, 2010.

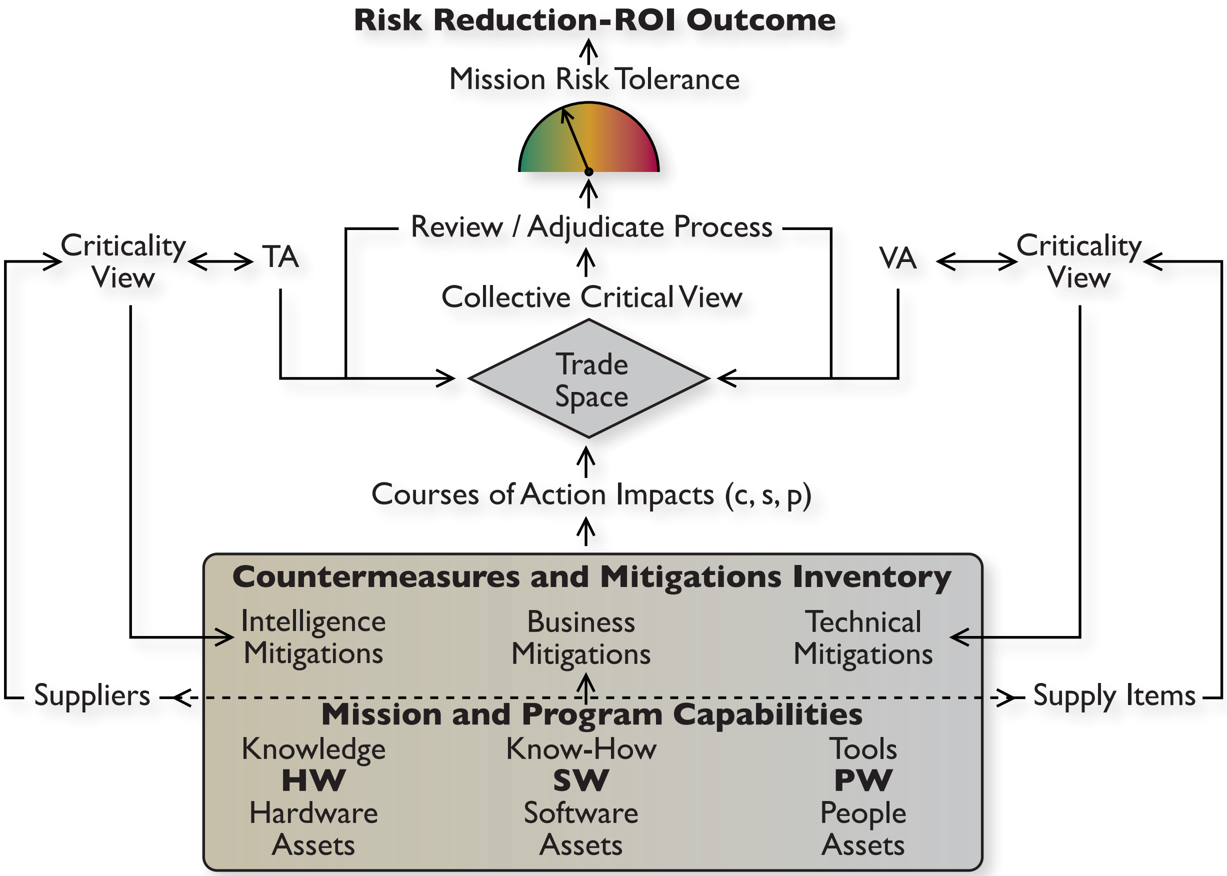

Figure 1. Supplier-Supply Chain Risk Management (S-SCRM) Enterprise Framework
(Illustration adapted from the paper Dr. Chan presented at the 2010 IEEE International Conference on Technologies for Homeland Security, Waltham, MA, November 8-10, 2010)

hardware, software, and people to implement a system. Intelligence mitigations are derived from conducting Threat Assessments (TAs); technical mitigations are derived from conducting vulnerability assessments (VAs); and business mitigations are derived from mission and program capabilities and best practices. These mitigations require a *collective critical view* to assess the cost (c), schedule (s), and performance (p) impacts in order to determine the best course of action. These impacts are the foundation upon which risk decisions are made to manage supplier and supply chain risks.

The IDA-developed enterprise framework for S-SCRM captures the underlying complexity and scope of concerns relevant to managing globalization and outsourcing effects of ICT risks. Using this framework, IDA is continuing research efforts to identify policies and processes to counter and mitigate threats to supply chains, to define priorities and ways to specify risk, and to assess the quality of RR-ROI decisions.

Dr. Chan is a research staff member in IDA's Information Technology and Systems Division. She holds a doctorate in engineering systems from the Massachusetts Institute of Technology.