CISQ
Consortium for IT Software Quality

ITAAC
INFORMATION TECHNOLOGY ACQUISITION ADVISORY COUNCIL

SUPPLY CHAIN RISK MANAGEMENT GETS LEGISLATIVE ATTENTION

JOE JARZOMBEK
Director for Government, Defense and Aerospace Programs, Synopsys

WILLIAM STEPHENS
Director of Counterintelligence, Defense Security Service

DON DAVIDSON
Deputy Director, Cybersecurity Risk Management (+ Chief of SCRM Division), Office of the Deputy DoD-CIO for Cybersecurity

SHON LYUBLANOVITS
Senior Advisor for Cybersecurity, GSA

DR. ALLAN FRIEDMAN
Director, Cybersecurity Initiatives, NTIA

Supply Chain Risk Management (SCRM) Gets Legislative Attention

- Moderator: Joe Jarzombek,
  - Director for Government, Defense and Aerospace Programs, Synopsys
  - Board Member, Consortium for IT Software Quality (CISQ)
- Panelists/Speakers:
- William Stephens, Director of Counterintelligence, Defense Security Service
- Don Davidson, Deputy Director, Cybersecurity Risk Management (+ Chief of SCRM Division), Office of the Deputy DoD-CIO for Cybersecurity (DoD)
- Shon Lyublanovits, Senior Advisor for Cybersecurity, Government Services Administration (GSA)
- Dr. Allan Friedman, Director, Cybersecurity Initiatives, National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce (DoC)

SCRM Guidance:
A Decade of Maturing Practices and Policy

- Efforts to manage risks associated with the cyber supply chain began in earnest with the **Comprehensive National Security Initiative (CNCI),** which was launched in 2008 with **National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23),** ***Cybersecurity Policy***
- **CNCI #11 ("Develop a multi-pronged approach for global supply chain risk management")** states that risks from both the domestic and global supply chains must be managed over the life cycle of a cyber-enabled component.

SCRM Guidance:
A Decade of Maturing Practices and Policy

- **Committee on National Security Systems (CNSS) Directive 505, *Supply Chain Risk Management*, was published in 2012 in accordance with CNCI Initiative #11.**
  - It states that the U.S. Government must address the reality that the global marketplace provides increased opportunities for adversaries to penetrate supply chains by establishing an organizational capability to identify and manage supply chain risk to national security systems.
  - Risks must be assessed early and throughout the acquisition life cycle, and all-source threat information must inform the use of risk mitigations.

SCRM Guidance:
A Decade of Maturing Practices and Policy

- Responding to the real possibilities of supply chain risk to critical systems, DoD issued two instructions to guide action.
  - **DoD Instruction 5200.39, *Critical Program Information (CPI) Protection*** *in DoD* and
  - **DoD Instruction 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN),*** 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).

NIST Special Publication & Interagency Report on *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*

- **NIST Special Publication (SP) 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*,** provides guidance to federal departments and agencies on identifying, assessing, and mitigating supply chain risk at all levels of their organizations using a multi-tiered SCRM-specific approach.
  - It integrates SCRM into federal agency risk management activities at all organizational levels and includes guidance on supply chain risk assessment and mitigation activities.
- **NIST Interagency Report (NISTIR) 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*** offers a set of practices that can be used for information systems categorized as high impact by Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*.
  - These practices are intended to promote the acquisition, development, and operations of information systems or systems of systems to meet cost, schedule, and performance requirements in today's environment, which is characterized by global suppliers and active adversaries.
  - NISTIR 7622 suggests risk mitigation strategies for various phases of the system development life cycle.

Office of Management and Budget (OMB) Circular A-130 (July 28, 2016) "*establishes general policy for the…acquisition, and management of Federal information, personnel, equipment, funds, IT resources and supporting infrastructure and services*."

Requirements of **A-130 "*apply to the information resources management activities of all agencies of the Executive Branch of the Federal Government*," and creates six specific requirements directly related to improving agencies' supply chain risk management (SCRM) capabilities.** As a matter of policy, A-130 requires agencies to:

- Consider "*supply chain security issues for all resource planning and management activities throughout the system development life cycle*;"
- "[A]*nalyze risks (including supply chain risks) associated with potential contractors and the products and services they provide,*" for all IT acquisitions; and
- "[A]*llocate risk responsibility between Government and contractor when acquiring IT*."

Office of Management and Budget (OMB) Circular A-130 (July 28, 2016) "*establishes general policy for the…acquisition, and management of Federal information, personnel, equipment, funds, IT resources and supporting infrastructure and services*." (continued)

Appendix I to A-130 "*establishes minimum requirements for Federal information security programs*." Appendix I requires agencies to:

- "[D]*evelop, implement, document, maintain, and oversee agency-wide information security and privacy programs*;" and
- **"[I]*mplement supply chain risk management principles to protect against the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software, as well as poor manufacturing and development practices throughout the system development life cycle*;"**

Section 4 of Appendix I gives requirements for "*those areas deemed to be of fundamental importance to the achievement of effective agency information security programs and those areas deemed to require specific emphasis by OMB*." Agencies are required to:

- **"[D]*evelop supply chain risk management plans as described in NIST SP 800-161 (SCRM Practices) to ensure integrity, security, resilience, and quality of information systems.*"**

SCRM Policy and practices not broadly implemented

Assertions of lack of funding associated with policy…

If you cannot afford to protect it, then you cannot afford to connect it.

Cost of loss and recovery from exploitation exceeds cost of protection.

Office of the Under Secretary of Defense, 19 Sep 2018 Memorandum on Class Deviation – Permanent SCRM Authority

252.239-7017 Notice of Supply Chain Risk (DEVIATION 2018-O0020).
Use the following provision, in lieu of the provision at DFARS 252.239-7017, in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items, for information technology, whether acquired as a service or as a supply, that is a covered system, is a part of a covered system, or is in support of a covered system, as defined at 239.7301 (DEVIATION 2018-O0020):

NOTICE OF SUPPLY CHAIN RISK (SEP 2018) (DEVIATION 2018-O0020)

(a) *Definition*. As used in this provision—

"Supply chain risk," means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system (see 10 U.S.C. 2339a).

(b) In order to manage supply chain risk, the Government may use the authorities provided by 10 U.S.C. 2339a. In exercising these authorities, the Government may consider information, public and non-public, including all-source intelligence, relating to an offeror and its supply chain.

(c) If the Government exercises the authority provided in 10 U.S.C. 2339a to limit disclosure of information, no action undertaken by the Government under such authority shall be subject to review in a bid protest before the Government Accountability Office or in any Federal court.

DHS Supply Chain Initiatives

- National Risk Management Center Supply Chain Task Force
- DHS RFI on Supply Chain Due-Diligence

SCRM Due-Diligence

- Exploitable weaknesses, known vulnerabilities and even malware can be embedded in software without malicious intent.
- Sloppy manufacturing hygiene is more often the cause of exploitable software. Such poor hygiene can be attributed to:
  - Lack of due care exercised by supply organizations with developers, integrators and testers who are often unaware of or untrained on software security, compounded by inadequate testing tools and the failure of suppliers to prioritize addressing the risks associated with the poor security of the software they deliver to the organizations that use it.

SCRM Due-Diligence

- For SCRM due-diligence to be sufficient, it requires more than understanding supplier pedigree and claims of process compliance; it requires third-party testing of software and software-controlled products, either by an independent lab or as part of acceptance testing by acquiring enterprises.
- Many tools and services find weaknesses and vulnerabilities in source code and binaries and also report a software bill of materials enumerating the open source components in both source and binary code files.
- At a minimum, there should be a requirement for suppliers to provide a bill of materials with test reports that provide evidence of mitigations associated with CWEs, CVEs and malware.
- Organizations not doing this as part of SCRM due-diligence are very much at risk of compromise and exploitation.

Supply Chain Risk Management (SCRM) Gets Legislative Attention

- Software supply chain assurance is finally ‘en vogue’.
- The Pentagon is evaluating how to insert security metrics into the acquisition process to measure cyber risk on the same scale as cost, schedule, and performance.
- This panel will discuss the latest developments, best practices, and standards of practice for SCRM.
  - “Deliver Uncompromised” as a focus to include Security in acquisition.
  - “Shift left,” referring to the practice of mitigating risk earlier in the system lifecycle to avoid costly, compounded technical debt and unacceptable levels of risk from vulnerabilities and compromise.
  - Etc.

Delivering Uncompromised (DU)

To deliver un-compromised war fighting capabilities to operating forces without critical information and/or technology being wittingly or unwittingly lost, stolen, denied, degraded or inappropriately given away or sold

- National Security, Defense, & Military, Strategies…
  - But **NO** Strategy to Secure Innovation — not valued/undervalued
- Threat **GREATEST** ever — highly contested environment
  - IC reporting, IC analysis, & Open Source supports
  - We are **NOT WINNING** — losses are profound
  - We've mapped methods of operation & points of contact
- What value is in our Innovation? — Is it worth protecting?
- Now is time to take back the initiative — ***"DU" is the GOAL!***

DU – How Might It Work?

- Tax Incentives; Litigation Reform; Insurance Market Reform; Contracts Warranties & Representations; International Norms

- Supplier Readiness Reform; Government Procurement Reform; Technology & Innovation