Supply Chain Risk Management (SCRM)

Ms. Jan Mulligan
ODASD(Logistics), Director of Supply
May 15, 2019
Agenda

• SCRM Definitions
  • DoDI 4140.01
  • Cyber Security
• SCRM Environment
• SCRM Communities of Practice
• Government SCRM Focus Areas
• ASD(Sustainment) SCRM Studies
• Sample Supply Chain Map
• DoD SCRM Way Forward
• Notional SCRM Governance Model
• What You Can Do
• Questions

POC: Ms. Jan Mulligan, ODASD(Logistics), 571-372-5227, Jan.b.mulligan.civ@mail.mil
Supply Chain Risk Management (SCRM) - The process for managing risk by identifying, assessing, and mitigating threats, vulnerabilities, and disruptions to the DoD supply chain from beginning to end to ensure mission effectiveness. Successful SCRM maintains the integrity of products, services, people, and technologies, and ensures the undisrupted flow of product, materiel, information, and finances across the lifecycle of a weapon or support system. **DoD SCRM encompasses all sub-sets of SCRM**, such as cybersecurity, software assurance, obsolescence, counterfeit parts, foreign ownership of sub-tier vendors, and other categories of risk that affect the supply chain.
Cyber Supply Chain Risk Management (C-SCRM) - the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of Information Technology (IT)/Operational Technology (OT) product and service supply chains. It covers the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction) as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an IT/OT product or service at any stage.

DoD C-SCRM is Usually Defined as Information and Communication Technology (ICT) Related to National Security Systems (NSS)

POC: Ms. Jan Mulligan, ODASD(Logistics), 571-372-5227, Jan.b.mulligan.civ@mail.mil
**SCRM Environment**

**Business threats**
- Supportability

**Adversary threats**
- Informational
- Disruptive

**Global Environment**

**Suppliers’ Environment**
(And outsource Manufacturing)

**Suppliers**

**Suppliers Facing**

**Organization’s Environment**

**Organization**

**Customer Facing**

**Customers’ Environment**

**Customers**

**Comprised of:** People, Material, Processes, Software, & Relationships

**Relationship Risk**
- Supplier Performance Risk
- Human Resource Risk
- Supply chain disruption risk
- Supplier Environment Risk
- Market Dynamics Risk
- Disaster Risk
- Political / Country Risk
- Supplier Financial Risk
- Regulatory Risk

**Operational Risk**
- Technical Risk
- Financial Risk
- Legal / Regulatory Risk
- Environmental Risk
- HR / Health and Safety Risk
- Political / Country Risk

**Financial Risk**
- Distribution Risk
- Relationship Risk
- Market Risk
- Brand / Reputation Risk
- Product Liability Risk
- Environmental Risk

**Political / Country Risk**

**POC:** Ms. Jan Mulligan, ODASD(Logistics), 571-372-5227, Jan.b.mulligan.civ@mail.mil
SCRM Communities of Practice

Working Representation of the Many COPs Across DoD SCRM

POC: Ms. Jan Mulligan, ODASD(Logistics), 571-372-5227,
Jan.b.mulligan.civ@mail.mil
<table>
<thead>
<tr>
<th>Document Name</th>
<th>Title</th>
<th>Type</th>
<th>Owner</th>
<th>Applies to</th>
<th>Topic</th>
<th>Applicability to SCRM</th>
</tr>
</thead>
<tbody>
<tr>
<td>NDAA Section 1639 (2018)</td>
<td>Measurement of Compliance with Cybersecurity Requirements for Industrial Control Systems</td>
<td>NDAA</td>
<td>Congress</td>
<td>DoD</td>
<td>Cybersecurity</td>
<td>Cyber scorecard for Industrial Control Systems</td>
</tr>
<tr>
<td>NDAA Section 807 (2018)</td>
<td>Process for Enhanced Supply Chain Scrutiny</td>
<td>NDAA</td>
<td>Congress</td>
<td>DoD</td>
<td>Risk Management</td>
<td>Stricter acquisition practices</td>
</tr>
<tr>
<td>NDAA Section 881 (2019) - Makes FY11 NDAA Section 806 Permanent</td>
<td>Permanent Supply Chain Risk Management Authority</td>
<td>NDAA</td>
<td>Congress</td>
<td>DoD</td>
<td>Acquisition/Cyber Risk Management</td>
<td>Information Communication Technology Risk to National Security Systems</td>
</tr>
<tr>
<td>DoDI 4140.01</td>
<td>DoD Supply Chain Materiel Management Policy</td>
<td>Instruction</td>
<td>USD(AT&amp;L)</td>
<td>DoD</td>
<td>Materiel Management</td>
<td>Materiel management across life cycle</td>
</tr>
<tr>
<td>DODI 5200.44</td>
<td>Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)</td>
<td>Instruction</td>
<td>USD(AT&amp;L)</td>
<td>CIO</td>
<td>TSN</td>
<td>Counterfeit/Integrity of Mission Critical Infrastructure</td>
</tr>
<tr>
<td>DoDI 8510.01</td>
<td>Risk Management Framework (RMF) for DoD Information Technology (IT)</td>
<td>Instruction</td>
<td>CIO</td>
<td>DoD</td>
<td>Cybersecurity</td>
<td>Cybersecurity platform for DoD, integrating information</td>
</tr>
</tbody>
</table>

POC: Ms. Jan Mulligan, ODASD(Logistics), 571-372-5227, Jan.b.mulligan.civ@mail.mil
• SCRM Study Phase I - Findings
  • Not organized to address SCRM holistically
  • Lack common definitions
  • Little information sharing

• SCRM Study Phase II - Recommendations
  • Devise a notional governance structure
  • Conduct vendor vetting & info sharing pilot
  • Pilot SCRM process and technology solutions

• Stakeholder feedback, independent studies, and Executive Orders agree with the conclusion that we can do better

• BLUF: We need to identify and address seams/gaps to secure our supply chains in a unified manner
Sample Supply Chain Map

72% of Tier 3 Suppliers reliant on Chinese Manufacturing

Assessment completed in days

Need to Better Understand Complex Vendor Support Structures
DoD SCRM Way Forward

• Potential Government Actions:
  • Establish our collective vision, goals, and objectives
  • Agree to organizational structures and approaches to SCRM solutions
  • Resource the effort

• Future Objectives:
  • Make SCRM easier for KOs to execute
  • Devise “pre-screening” strategies for vendors
  • Leverage and incentivize industry to protect supply chains
  • Consider process resiliency in addition to system resiliency
  • Look at more than ACAT I systems
  • Develop impact legislation and policy
  • Bridge the threat classification gap to enable SCRM

POC: Ms. Jan Mulligan, ODASD(Logistics), 571-372-5227, Jan.b.mulligan.civ@mail.mil
What You Can Do

- Understand Acq and Sustainment are Two Points on Same Continuum
- Create Agile LCSP’s to Address Eventual Obsolescence
- Understand Where Risk is Acceptable
- Share Information on Risks Discovered in Your Program
- Conduct Due Diligence on Understanding Lower Tiers of Supply Chain
- Plan for Eventual Disruption to Your Supply Chain
- Use Best Practices … No Need to Duplicate Effort of Others
- Make PPP’s & LCSP’s Living Documents
- Practice Good Cyber Hygiene, and Recognize Threats
- Train and Exercise Your Organization to be Resilient

POC: Ms. Jan Mulligan, ODASD(Logistics), 571-372-5227, Jan.b.mulligan.civ@mail.mil
QUESTIONS?