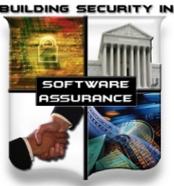


# Supply Chain Risk Management: Enabling Transparency for Informing Decision- Making in Reducing Residual Risk Exposures

Joe Jarzombek, PMP, CSSLP  
Director for Software Assurance  
Cyber Security & Communications  
US Department of Homeland Security

**DHS SCRM and SwA (Software SCRM) Program Offices**





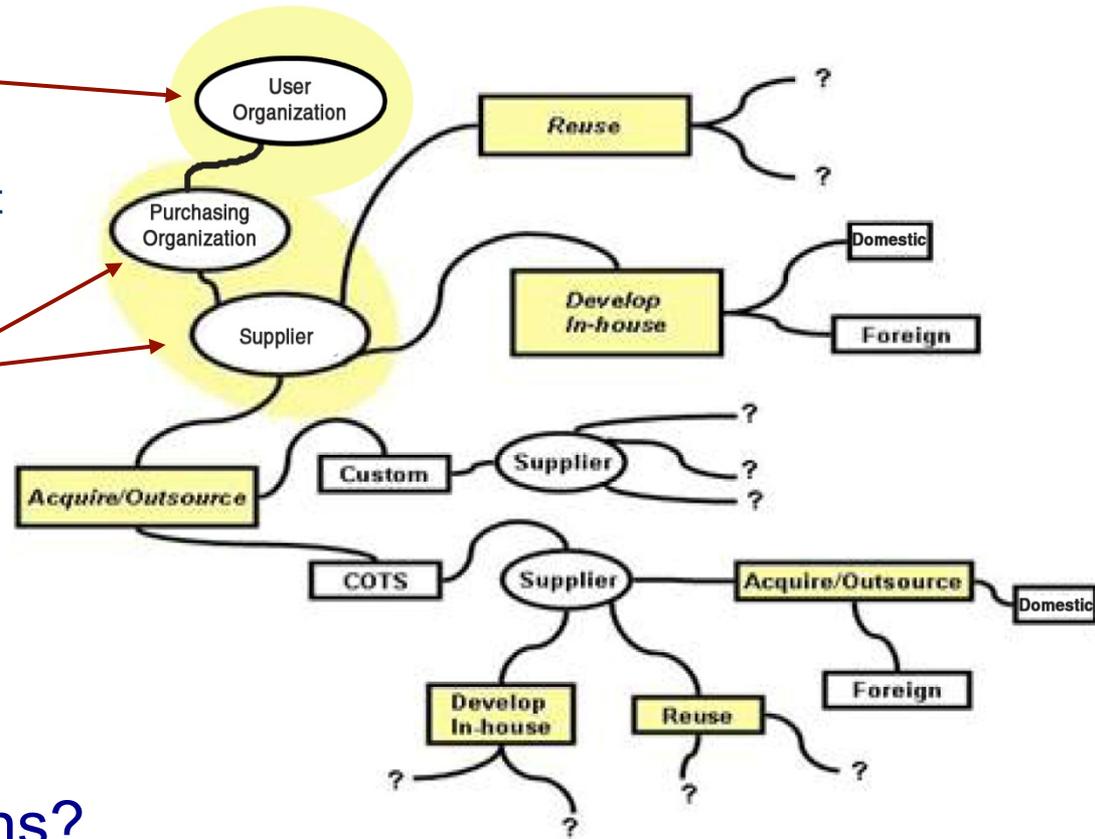
# Risk Management (Enterprise ↔ Project): Shared Processes & Practices ↔ Different Focuses

## ▶ Enterprise-Level:

- Regulatory compliance
- Changing threat environment
- Business Case

## ▶ Program/Project-Level:

- Cost
- Schedule
- Performance



Who makes risk decisions?

Who “owns” residual risk from tainted/counterfeit products?

\* “Tainted” products are those that are corrupted with malware, or exploitable weaknesses & vulnerabilities that put users at risk



# Challenges in Mitigating Risks Attributable to Exploitable Software and Supply Chains (cont.)

Enterprises seek comprehensive capabilities to:

- ▶ Avoid accepting software with **MALWARE** pre-installed. **MAEC**
- ▶ Determine that no publicly reported **VULNERABILITIES** remain in code prior to operational acceptance, and that future discoveries of common vulnerabilities and exposures can be quickly patched. **CVE**
- ▶ Determine that exploitable software **WEAKNESSES** that put the users most at risk are mitigated prior to operational acceptance or after put into use (and not previously evaluated for exploit potential). **CWE**

# DHS/NPPD/SCRM Work Program

## 1. Protect Critical Infrastructure

- 1.1 **Build partnership** with private sector telecomm and IT companies to address SCRM (DHS)
- 1.2 Develop and pilot a “**transaction awareness process**” to help private sector acquisition security (DHS)
- 1.3 **Augment USG procurement** of ICT equipment and services, to give USG system owners authority to require SCRM in response to emerging threats (GSA)
- 1.4 Understand communications circuitry that supports **Primary Mission Essential Functions (PMEF)** and develop risk management (OSTP & DOD)
- 1.5 Consider **new legislative authorities** to regulate SCRM across dependent sectors (DOD & DOC)
- 1.6 Develop **multi-tiered, standards-driven approach** to standards-based risk management frameworks for SCRM (NIST & DHS & FCC)
- 1.7 **Fund transition of critical technologies** into domestic, sustainable production capabilities (OSTP & DPAC)

## 2. Bridge Security/Acquisition Gaps

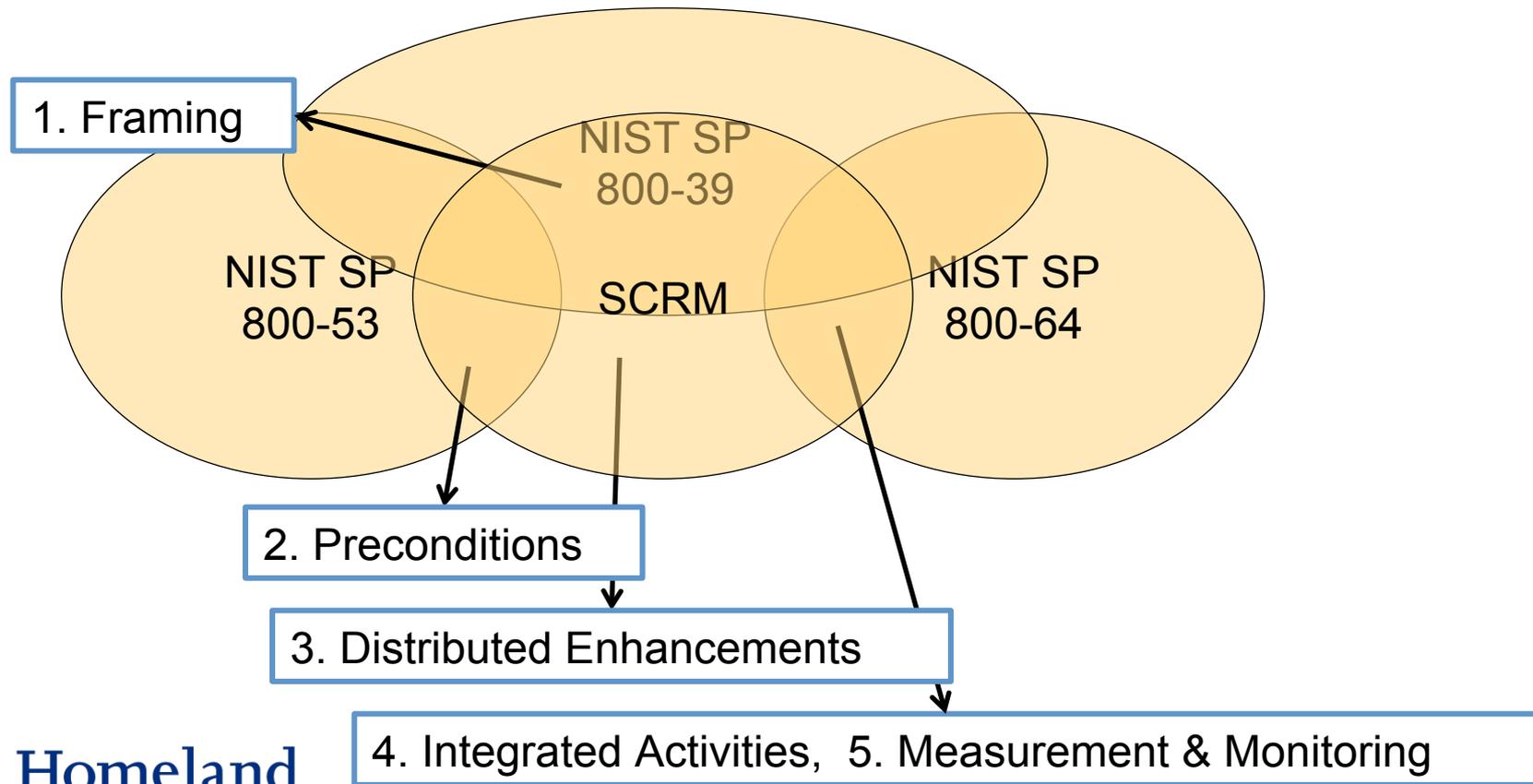
- 2.1 **Develop frame of reference** for common discussion of SCRM threats, acquisition gaps, security measures. Develop and pilot analytic processes for evaluating SCRM.
- 2.2 **Develop SCRM analytic tools** for implementing SCRM consistently across D/As (including domain specific acquisition support, text analytics, risk-based decision support, forensics)
- 2.3 **Provide sample contract language and track** successful implementations in database for SCRM tool enhancements, or for promulgation of best practices
- 2.4 Support the development of **SCRM policies, procedures, and governance** for the implementation and monitoring of SCRM across civilian D/As
- 2.5 Develop operations for **detection, forensics, incident response** in collaboration with US-CERT and the NCCIC
- 2.6 Build relationships **with acquisition groups** and pilot SCRM tools, evaluate success, and continuously improve



**Homeland  
Security**

# Objectives

- Need “systems-of-systems” or “enterprise systems” thinking for risk management (building on 800-39 and 800-64)
- IT Baselines for SCRM are different, but should build on 800-53
- Need consistency of terms



# Practical Steps

## 1. Frame supply chain risk at all levels of the enterprise

- Broaden 800-39 to include systems engineering and acquisition lifecycles
- Deepen 800-39 to elaborate on supply chain threats/risks

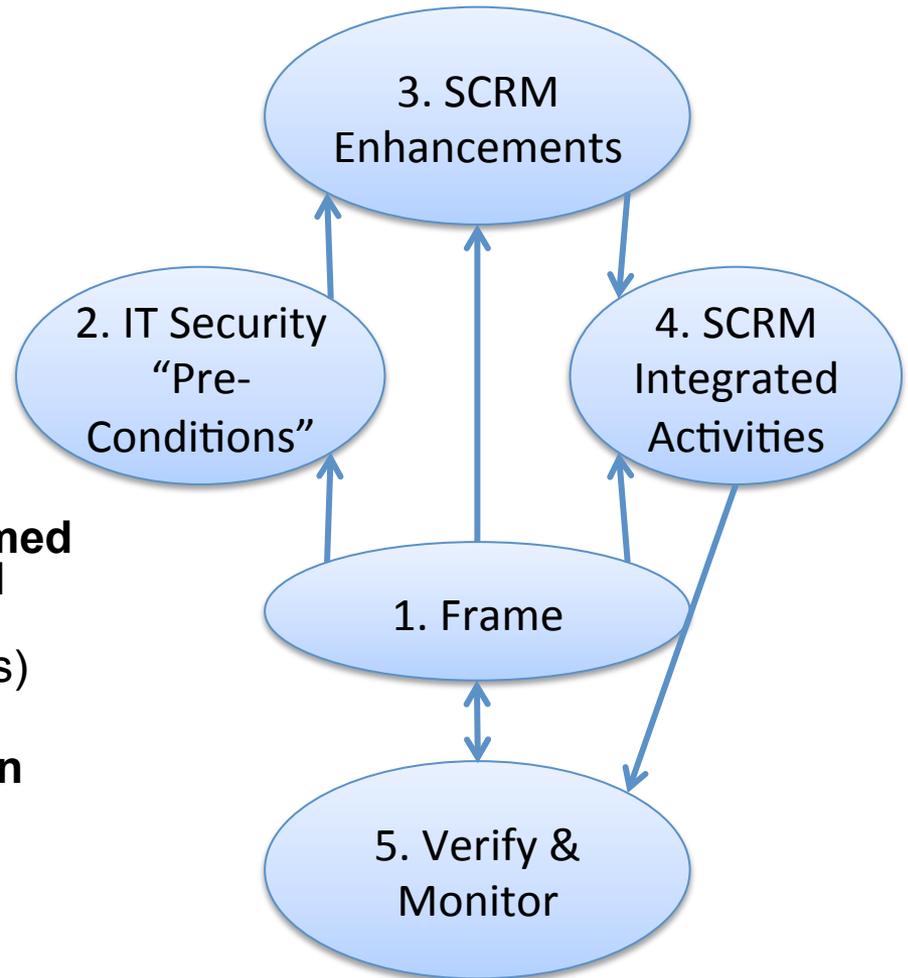
## 2. Set IT baselines for SCRM

- 800-53 baselines are defined for general IT system, but connectivity and adverse marketplace might require different baseline for effective SCRM

## 3. Define SCRM enhancements performed autonomously by various functional groups (e.g., physical security, IA, software assurance, suppliers, logistics)

## 4. Define integrated activities across systems engineering and acquisition lifecycles

## 5. Measure and monitor effectiveness



# Step 1 – Frame SCRM

## Adapt NIST 800-39 guidance:

1. the multi-tiered organization views and process elements must be elaborated upon for the integrated organization for SCRM (**greater depth into supply chains**), and
2. the risk management features must be expanded to account for non-traditional IT operations (**greater breadth to include development/acquisition operations and logistics**).

## Example Elaborations:

### Tier One – Organization/Enterprise View

- **Governance and Risk Executive** includes integrated structure for IT, security, logistics, contracting, and so forth
- **Risk Management Strategy** frames supply chain threats and vulnerabilities (in both products and processes)
- **Investment Strategies** include secure replacement of exploitable modules

### Tier Two – Mission/Business View

- **Risk Awareness** includes supply chain concerns, such as tainted and counterfeit products
- **Enterprise/Infosec Architecture** include development lifecycles and contracting details

### Tier Three – Information System View

- Appropriate activities built in across **lifecycle phases** (e.g., development, acquisition, sustainment, operations)



**Homeland  
Security**

\* “Tainted” products are those that are corrupted with malware, or exploitable weaknesses & vulnerabilities that put users at risk

# Step 1 – Frame SCRM

Need a common Risk Frame of Reference to ground enterprise-, mission-, and system-focused processes

Supply Chain Threats Cause Risk

**Acquisition Weaknesses**  
(Business & Technical Threat-Enabling Behaviors)

**Supply Chain Exploits** (Activities in the Supply Chain Causing Impact on Business or Mission)

**Threatening Activities**  
(Company/Marketplace Activity Might Indicate Threat Likelihoods)

**Collaboration** Across Functional Groups at Key Decision Points Strengthens Acquisition

**Countermeasure Selection** of Based on Business Impact Cost-Effectively Deters Exploits

**Indicators** about Companies and Marketplace Activity Indicates Likelihood to Improve Risk Awareness and Decisions

*\*Need SCRM & SwA 'standard' definitions*

Mitigations Reduce Risk

Failure to Ship  
Theft / Destruction  
Examination / Disclosure  
Substitution (incl Gray Market)  
Alteration / Malware  
Theft / Destruction  
Examination / Disclosure  
Substitution (incl Gray Market)  
Alteration / Malware  
Theft / Destruction  
Examination / Disclosure  
Substitution (incl Gray Market)  
Alteration / Malware

Within Trusted Custody prior to Final Shipment

In Transit or En Route Storage

Within Trusted Acquirer after Final



**Homeland Security**

*\* to unambiguously enable contract supplier-acquirer-user relationships*

# Steps 2 thru 4 – Select SCRM Practices

- Select “key practices” based on risk-informed processes developed in the supply chain risk framing step
- Reorganize into three sections:
  - Preconditions – minimum that must be in place for successful SCRM
  - Distributed Enhancements – additional preconditions to be implemented by specific security disciplines (e.g., physical security, information security)
  - Integrated Activities – define how SCRM is established between disciplines throughout system lifecycle

## System Lifecycle



2. Preconditions
<ol style="list-style-type: none"> <li>1. Identification and Authentication</li> <li>2. Access Control</li> <li>3. Configuration Management</li> <li>4. Awareness and Training</li> <li>5. Physical and Env. Protection</li> </ol>

	Initiation	Development/ Acquisition	Implementation/ Assessment	Operations/ Maintenance	Disposal
3. Distributed Enhancements	<ol style="list-style-type: none"> <li>1. Establish secure disposal procedures</li> <li>2. Establish alternate routes of information sharing</li> </ol>	<ol style="list-style-type: none"> <li>1. Verify compliance with requirements</li> <li>2. Identify mission-critical system elements</li> </ol>	<ol style="list-style-type: none"> <li>1. Assess security of physical and logical implementation</li> <li>2. Ensure that system remains operational during maintenance</li> </ol>	<ol style="list-style-type: none"> <li>1. Prevent unnecessary information sharing</li> </ol>	<ol style="list-style-type: none"> <li>1. Ensure final disposal procedures match significance of system</li> </ol>
4. Integrated Activities	<ol style="list-style-type: none"> <li>1. Supply chain diversity</li> <li>2. Develop counter-measures</li> </ol>	<ol style="list-style-type: none"> <li>1. Check for tampering throughout process</li> <li>2. Verify predictability under stress</li> </ol>	<ol style="list-style-type: none"> <li>1. Examine consequences of system compromise</li> <li>2. Prepare and test counter measures</li> </ol>	<ol style="list-style-type: none"> <li>1. Update counter-measures as threats develop</li> <li>2. Implement updates without disrupting operations</li> </ol>	<ol style="list-style-type: none"> <li>1. Ensure disposal of all parts no longer in use</li> </ol>



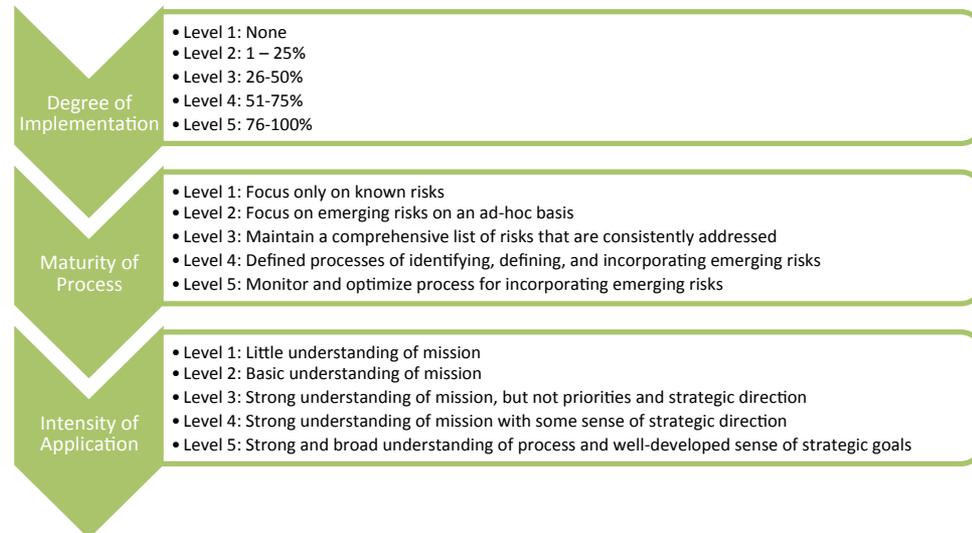
# Step 5 – Measure, Monitor, and Reprioritize Practices (Especially for Visibility, Understanding, and Control)

- To assess effectiveness of SCRM policy, it is necessary to identify measurable outcomes of SCRM, as well as the level of implementation
- Measurement framework would serve as a foundation for understanding and improving SCRM practices

## Example Outcomes

Risk Understanding	Interagency Partner Engagement	Contracting
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Confidence in the quality of risk-related data	<input type="checkbox"/> Ability to describe risks to senior business leaders	<input type="checkbox"/> Firm knowledge of the controls portfolio in place at major contractors
<input type="checkbox"/> Ability to use risk estimates in investment decisions	<input type="checkbox"/> Ability to persuade interagency partners to make decisions based on risk information	<input type="checkbox"/> Ability to describe the risk landscape of major contractors
<input type="checkbox"/> Ability to identify significant new risks	<input type="checkbox"/> Clear understanding of who holds responsibility for addressing control gaps	<input type="checkbox"/> Contractors understand requirements necessary to comply with regulations
<input type="checkbox"/> Ability to assess protection levels against newly identified threats	<input type="checkbox"/> Interagency partners understand their responsibilities in managing risk	<input type="checkbox"/> Contractors have confidence in ability to satisfy regulatory requirements and address gaps
<input type="checkbox"/> Ability to effectively prioritize gaps for remediation	<input type="checkbox"/> Interagency partners understand risk data	<input type="checkbox"/> Contractors have confidence that information on configurations of controls is current and accurate
	<input type="checkbox"/> Interagency partners actively manage and close risks independently	<input type="checkbox"/> Contractors have the ability to anticipate new regulations and requirements
	<input type="checkbox"/> Interagency partners willingly and formally accept residual risks	

## Example Levels of Implementation



# Supply Chain Risk Management: Enabling Transparency for Informing Decision- Making in Reducing Residual Risk Exposures



# Homeland Security

# SOFTWARE ASSURANCE FORUM



Homeland  
Security

## BUILDING SECURITY IN



Commerce



National  
Defense

Public/Private Collaboration Efforts for  
Security Automation and Software  
Supply Chain Risk Management



Next SwA Working Groups sessions: 27-29 Nov 2012 at MITRE, McLean, VA