AF Cyber- Supply Chain Risk Management

Alyssa Feola, SAF/CNZP
Senior Cybersecurity Advisor
Cyber Supply Chain Risk Management (C-SCRM) Technical Lead
12 August 2019
Cyber Supply Chain Risk Management remains a hard problem.

- Globalized markets which can be influenced by foreign adversaries
- Continued growth in complexity of Information and Communications Technology (ICT)
- Increase in the number of entities who interact with products and services
- Lack of visibility and understanding of the supply chain
- Lack of guidance and tools for supply chain risk decisions

SCRM Threats in the news...

- Supply chain attacks spiked 78% from 2017 to 2018 (Symantec's 2019 Threat Report),... increasingly exploiting vulnerabilities in commercial software and operating systems to launch downstream cyberattacks.
- Two-thirds of respondents reported that their organizations had experienced a software supply chain attack, and 90% of those confirmed they had incurred financial cost averaging over $1.1 million in damage.
Support for a vibrant domestic manufacturing sector, a solid defense industrial base, and resilient supply chains is a national priority.

Resilient and agile logistics. Ensure logistics sustainment while under persistent multi-domain attack.

Establish a process for enhancing scrutiny of acquisition decisions in order to improve the integration of SCRM.
As ICT has evolve, so has AF’s approach to SCRM:

- Focus on risk in acquisition decisions...
  - Traditional focus on cost, performance, and schedule (get it cheap, cast, and working)
  - Increase focus on cybersecurity as a critical risk factor (get it secure)

- The right governance, risk, and compliance frameworks established to
  - Identify assets in the inventory
  - Get threat information to the appropriate decision-makers
  - Carry out the activities necessary
Purpose: The AF SCRM charter establishes the scope of work and authorities for implementing comprehensive Supply Chain Risk Management (SCRM) across the Air Force.

Governance Structure: Establish a cross-functional team to gain AF-enterprise executive-level support focused on security to enable intra-agency collaboration to recognize, assess, and mitigate supply chain risks and prevent supply chain disruptions.

Duties and Responsibilities: AF-enterprise SCRM requires continual feedback and connection between various agencies to ensure intelligence-informed horizontal protection and reporting. Agencies involved include DIA SCRM TAC, AFOSI, SAF/AA, SAF/AQ, SAF/CN, SAF/GC, SAF/IA, AF/A2, AF/A4, AF/A6, AFMC, ACC and other MAJCOMs.

SAF CIO Focus:
- Align C-SCRM activity with RMF process
- Integrate C-SCRM with Secure Systems Engineering
- Right amount of security based on system management
  - Cybersecurity Testing and Engineering procedures
  - Sustainment and Maintenance throughout Life Cycle

---

**AF SCRM Governance & AF C-SCRM Focus**

- **Purpose:** The AF SCRM charter establishes the scope of work and authorities for implementing comprehensive Supply Chain Risk Management (SCRM) across the Air Force.

- **Governance Structure:** Establish a cross-functional team to gain AF-enterprise executive-level support focused on security to enable intra-agency collaboration to recognize, assess, and mitigate supply chain risks and prevent supply chain disruptions.

- **Duties and Responsibilities:** AF-enterprise SCRM requires continual feedback and connection between various agencies to ensure intelligence-informed horizontal protection and reporting. Agencies involved include DIA SCRM TAC, AFOSI, SAF/AA, SAF/AQ, SAF/CN, SAF/GC, SAF/IA, AF/A2, AF/A4, AF/A6, AFMC, ACC and other MAJCOMs.

**SAF CIO Focus:**
- Align C-SCRM activity with RMF process
- Integrate C-SCRM with Secure Systems Engineering
- Right amount of security based on system management
  - Cybersecurity Testing and Engineering procedures
  - Sustainment and Maintenance throughout Life Cycle

---

**AF SCRM Governance & AF C-SCRM Focus**

- **Purpose:** The AF SCRM charter establishes the scope of work and authorities for implementing comprehensive Supply Chain Risk Management (SCRM) across the Air Force.

- **Governance Structure:** Establish a cross-functional team to gain AF-enterprise executive-level support focused on security to enable intra-agency collaboration to recognize, assess, and mitigate supply chain risks and prevent supply chain disruptions.

- **Duties and Responsibilities:** AF-enterprise SCRM requires continual feedback and connection between various agencies to ensure intelligence-informed horizontal protection and reporting. Agencies involved include DIA SCRM TAC, AFOSI, SAF/AA, SAF/AQ, SAF/CN, SAF/GC, SAF/IA, AF/A2, AF/A4, AF/A6, AFMC, ACC and other MAJCOMs.

**SAF CIO Focus:**
- Align C-SCRM activity with RMF process
- Integrate C-SCRM with Secure Systems Engineering
- Right amount of security based on system management
  - Cybersecurity Testing and Engineering procedures
  - Sustainment and Maintenance throughout Life Cycle

---

**AF SCRM Governance & AF C-SCRM Focus**

- **Purpose:** The AF SCRM charter establishes the scope of work and authorities for implementing comprehensive Supply Chain Risk Management (SCRM) across the Air Force.

- **Governance Structure:** Establish a cross-functional team to gain AF-enterprise executive-level support focused on security to enable intra-agency collaboration to recognize, assess, and mitigate supply chain risks and prevent supply chain disruptions.

- **Duties and Responsibilities:** AF-enterprise SCRM requires continual feedback and connection between various agencies to ensure intelligence-informed horizontal protection and reporting. Agencies involved include DIA SCRM TAC, AFOSI, SAF/AA, SAF/AQ, SAF/CN, SAF/GC, SAF/IA, AF/A2, AF/A4, AF/A6, AFMC, ACC and other MAJCOMs.

**SAF CIO Focus:**
- Align C-SCRM activity with RMF process
- Integrate C-SCRM with Secure Systems Engineering
- Right amount of security based on system management
  - Cybersecurity Testing and Engineering procedures
  - Sustainment and Maintenance throughout Life Cycle

---

**AF SCRM Governance & AF C-SCRM Focus**

- **Purpose:** The AF SCRM charter establishes the scope of work and authorities for implementing comprehensive Supply Chain Risk Management (SCRM) across the Air Force.

- **Governance Structure:** Establish a cross-functional team to gain AF-enterprise executive-level support focused on security to enable intra-agency collaboration to recognize, assess, and mitigate supply chain risks and prevent supply chain disruptions.

- **Duties and Responsibilities:** AF-enterprise SCRM requires continual feedback and connection between various agencies to ensure intelligence-informed horizontal protection and reporting. Agencies involved include DIA SCRM TAC, AFOSI, SAF/AA, SAF/AQ, SAF/CN, SAF/GC, SAF/IA, AF/A2, AF/A4, AF/A6, AFMC, ACC and other MAJCOMs.

**SAF CIO Focus:**
- Align C-SCRM activity with RMF process
- Integrate C-SCRM with Secure Systems Engineering
- Right amount of security based on system management
  - Cybersecurity Testing and Engineering procedures
  - Sustainment and Maintenance throughout Life Cycle

---

**AF SCRM Governance & AF C-SCRM Focus**

- **Purpose:** The AF SCRM charter establishes the scope of work and authorities for implementing comprehensive Supply Chain Risk Management (SCRM) across the Air Force.

- **Governance Structure:** Establish a cross-functional team to gain AF-enterprise executive-level support focused on security to enable intra-agency collaboration to recognize, assess, and mitigate supply chain risks and prevent supply chain disruptions.

- **Duties and Responsibilities:** AF-enterprise SCRM requires continual feedback and connection between various agencies to ensure intelligence-informed horizontal protection and reporting. Agencies involved include DIA SCRM TAC, AFOSI, SAF/AA, SAF/AQ, SAF/CN, SAF/GC, SAF/IA, AF/A2, AF/A4, AF/A6, AFMC, ACC and other MAJCOMs.

**SAF CIO Focus:**
- Align C-SCRM activity with RMF process
- Integrate C-SCRM with Secure Systems Engineering
- Right amount of security based on system management
  - Cybersecurity Testing and Engineering procedures
  - Sustainment and Maintenance throughout Life Cycle

---

**AF SCRM Governance & AF C-SCRM Focus**

- **Purpose:** The AF SCRM charter establishes the scope of work and authorities for implementing comprehensive Supply Chain Risk Management (SCRM) across the Air Force.

- **Governance Structure:** Establish a cross-functional team to gain AF-enterprise executive-level support focused on security to enable intra-agency collaboration to recognize, assess, and mitigate supply chain risks and prevent supply chain disruptions.

- **Duties and Responsibilities:** AF-enterprise SCRM requires continual feedback and connection between various agencies to ensure intelligence-informed horizontal protection and reporting. Agencies involved include DIA SCRM TAC, AFOSI, SAF/AA, SAF/AQ, SAF/CN, SAF/GC, SAF/IA, AF/A2, AF/A4, AF/A6, AFMC, ACC and other MAJCOMs.

**SAF CIO Focus:**
- Align C-SCRM activity with RMF process
- Integrate C-SCRM with Secure Systems Engineering
- Right amount of security based on system management
  - Cybersecurity Testing and Engineering procedures
  - Sustainment and Maintenance throughout Life Cycle
AF C-SCRM: NIST ICT SCRM Framework - Frame

Step 1 of 4: Frame

- **Tasks:**
  1.1 Determine Baseline Criticality
  1.2 Develop ICT SCRM Policy
  1.3 Integrate ICT SCRM considerations into enterprise Risk management

- **Activities:**
  - USAF Guide - Critical Program Information & Critical Component
  - Policy – AFI 17-130, AFI 63-101/20-101
  - Establish risk tolerance and threshold

Related AF SCRM Objective

1. Approach
2. Alignment
3. Intelligence
4. Culture
5. Coordination
6. Tools
Step 2 of 4: Assess

- **Tasks:**
  2.1 Integrate ICT SCRM Considerations into enterprise risk management

- **Activities:**
  - AF SCRM WG under AFSEEB
    - AF C-SCRM WG aligns to Risk Executive Function

**Related AF SCRM Objective**

1. Approach
2. Alignment
3. Intelligence
4. Culture
5. Coordination
6. Tools
Step 3 of 4: Respond

- **Tasks:**
  1. Make enterprise risk decisions to avoid, mitigate, share, or transfer risk
  2. Select, tailor & implement appropriate enterprise ICT SCRM controls
  3. Document controls in Enterprise ICT SCRM Plan

- **Activities:**
  - Functional based response activity
  - Enterprise/Organization/System Risk tolerance Baseline
  - AF SCRM Plan

**Related AF SCRM Objective**

1. Approach
2. Alignment
3. Intelligence
4. Culture
5. Coordination
6. Tools
Step 4 of 4: Monitor

Tasks:
- 3.1 Integrate ICT SCRM into agency Continuous Monitoring program
- 3.1 Monitor and evaluate enterprise-level constraints and risks for change and impact
- 3.1 Monitor effectiveness of enterprise-level risk response

Activities:
- AF Continuous Monitoring Strategy
- AF Cyberspace Operations
- AF C-SCRM WG

Related AF SCRM Objective
1. Approach
2. Alignment
3. Intelligence
4. Culture
5. Coordination
6. Tools
Path to better supply chain risk management:

- Continue to build off the success and lessons learned within the AF Enterprise
- Continue to partner and support national initiatives
- Exercise C-SCRM authorities
- Expand C-SCRM outreach - Authorizing Officials, Program Managers, etc
- Foster Cyber Supply Chain Due Diligence based on risk
  - Develop actionable cyber supply chain implementation guidance
  - Advocate the use of commercial SCRM intelligence tools by procurement officers, AOs, Program Managers to enable appropriate due diligence
  - Promote the illumination and assessment of the supply chain through the use of automated commercial SCRM capabilities and services:
    - Supply Chain Mapping
    - Supply Chain Risk Assessments
    - Supply Chain Continuous Monitoring and reporting
- Develop decision tools to support risk analysis and risk management, including an products assessment list