Supply Chain Risk Management (SCRM)

Brian S. Cohen
703-845-6684, bcohen@ida.org

October 31, 2017

This material represents ongoing technical work and the views of the author and does not necessarily represent any policies or positions of the government
Five categories for improvement

1. Understand supply chain risk
   - Expand vulnerability assessments

2. Mitigate potential vulnerabilities
   - Improve detection and reporting

3. Approach acquisition differently
   - Enhance program protection planning
   - Improve timeliness of supplier vetting
   - Improve system engineering
   - Use JFAC and JAPEC effectively
   - Consider cybersecurity impact of COTS products and components

4. Support life-cycle operations
   - Establish sustainment PPPs for fielded systems
   - Collect and act on parts vulnerabilities

5. Pursue technical solutions

Publicly-released report published Feb 2017
Available at: http://www.acq.osd.mil/dsb/reports/2010s/DSBCyberSupplyChain_ExecSummary_Distribution_A.PDF

Source: Engineering Cyber Resilient Weapon Systems, Kristen Baldwin, SAE Aerotech Congress, Unclassified, September 27, 2017
What Are We Protecting

Program Protection & Cybersecurity
DoDI 5000.02, Enclosure 3 & 14

Technology

**What:** A capability element that contributes to the warfighters’ technical advantage (Critical Program Information (CPI))

**Key Protection Activity:**
- Anti-Tamper
- Defense Exportability Features
- CPI Protection List
- Acquisition Security Database

**Goal:** Prevent the compromise and loss of CPI

Components

**What:** Mission-critical functions and components

**Key Protection Activity:**
- Software Assurance
- Hardware Assurance/Trusted Foundry
- Supply Chain Risk Management
- Anti-counterfeits
- Joint Federated Assurance Center (JFAC)

**Goal:** Protect key mission components from malicious activity

Information

**What:** Information about the program, system, designs, processes, capabilities and end-items

**Key Protection Activity:**
- Classification
- Export Controls
- Information Security
- Joint Acquisition Protection & Exploitation Cell (JAPEC)

**Goal:** Ensure key system and program data is protected from adversary collection

Protecting Warfighting Capability Throughout the Lifecycle

Policies, guidance and white papers are found at our initiatives site: http://www.acq.osd.mil/se/initiatives/init_pp-sse.html

Source: Engineering Cyber Resilient Weapon Systems, Kristen Baldwin, Cleared - Case # 17-S-1176, SAE Aerotech Congress, September 27, 2017
Program Protection Planning (PPP)

• Includes all the Program Protect Disciplines
• Programs should create a PPP that supports the entire LifeCycle
• Should feed into and be Maintained through Sustainment
• PPPs are reviewed by DOD
• PPPs are a “plan”
  o Programs have options on implementation
  o Contractors primarily offer “mitigations” and “solutions” for implementation
• SCRM in the context of the PPP is about “Malicious” exploitation and the “Cyber” risk

Program Protection Plan Outline and Guidance, DASD(SE), July 2011
Why is LifeCycle SCRM Hard?

• Risk = Function (Threat, Vulnerability, Consequence)
  o Consequence – How Serious Is Impact On System/Mission?
  o Vulnerability – How Readily Will A Component Compromise Cause A Consequence
  o Criticality = Function (Consequence And Vulnerability)
  o Threat – Adversary Motivation, Capability And Access
  o Obsolescence Threat - Easy Access And Little Capability Needed Introduce Bad Parts

• Acquisition Programs Have Great Knowledge About Critical Components, But Little Knowledge About Sustainment Threat

• Sustainment Has Detailed Knowledge About Obsolescence Threat, But Little Knowledge About Criticality

• Recent Revisions To DoDM 4140.01 Volume 11 Should Help Remedy This (At Least For New Programs)
Program Protection Integrated into Policy

DoDI 5000.02 Operation of the Defense Acquisition System
- Regulatory Requirement for Program Protection Plan at Milestones A, B, C and FRP/FDD

DoDI 5200.39 Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)
- Assigns responsibility for Counterintelligence, Security, and System Engineering support for the ID and protection of CPI
- Rescoped definition of CPI

DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks
- Establishes policy and responsibilities to minimize the risk that warfighting capability will be impaired due to vulnerabilities in system design or subversion of mission critical functions or components

DoDI 4140.67 DoD Counterfeit Prevention Policy
- Establishes policy and assigns responsibility to prevent the introduction of counterfeit material at any level of the DoD supply chain

DoDI 8500.01 Cybersecurity
- Establishes policy and assigns responsibilities to achieve DoD cybersecurity through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare

Source: Cybersecurity and Program Protection, 2016 NDIA SE Conference, Melinda K. Reed, Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0039. Distribution is unlimited, October 24, 2016
• 5200.44 Defines the Supply Chain Risk Management (SCRM) Policy

• What does it say about Microelectronics? (Policy Section 4)
  o C. Manage risk to critical functions and components by:
    ▪ Reducing vulnerabilities ....
    ▪ Apply quality, configuration and security practices, with special attention to military end-use products and services
    ▪ Anti - Counterfeit Measures
    ▪ Detect Vulnerabilities in Custom and OTS products
  
  o E. ...Custom integrated circuit-related products and services shall be procured from a trusted supply chain

Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)
How to Implement Policy

• All depend on TSN Risk Analysis

• Assessment and Mitigations Are in Three “Lanes”
  o Anti-Counterfeit Measures
  o Use of Trusted Suppliers for ASICs
  o Hardware and Software Assurance (HwA and SwA) – including the use of the Joint Federated Assurance Centers (JFAC)

• Anti-Counterfeit
  o Use Original Component Manufacturer Authorized Distributor, Use Counterfeit Screening (i.e. AS5553) if possible

Trusted Systems and Networks (TSN) Analysis, June 2014
Additional Guidance in the Defense Acquisition Guidebook (DAG Chapter 9) - Program Protection (PDF Version)
TSN Methodology

Criticality Analysis → Consequence of Loss → Likelihood of Loss → Risk Assessment

Threat Assessment → Vulnerability Assessment

Identification of Potential Countermeasures

- Options
  - Prevent CMs
  - Detect CMs
  - Respond CMs

Trade-off Analysis → Risk Mitigation Decisions

Countermeasure (CM) Selection

Risk Assessment

Consequence

- Initial Risk
- Mitigated Risk

Source: Program Protection Implementation Considerations, 2014 NDIA Program Protection Summit, Melinda Reed, Distribution Statement A – Approved for public release by DOPSR on 5/14/14; Case #14-S-1578 applies. Distribution is unlimited, May 21, 2014
The Trusted Foundry Program (TFP) was established as a joint effort between Department of Defense and National Security Agency . . . in response to Deputy Secretary of Defense Paul Wolfowitz’s 2003 Defense Trusted IC Strategy memo.

By the end of FY2017, DoD will have invested >$850M for leading-edge microelectronics access and services including manufacturing for a wide array of weapon systems devices with feature sizes down to 14nm on 300 mm wafers.

It was soon recognized a broader supply chain was needed and the program was broadened to include other microelectronics suppliers to increase competition and ensure the entire supply chain could be trusted.

The TFP provides national security and defense programs with access to state of the art semiconductor integrated circuits from secure sources.
• Trusted supplier accreditation plan expanded the ranks of suppliers capable of providing trusted services for leading-edge, state-of-the-practice and legacy parts by certifying that suppliers meet a comprehensive set of security and operations criteria.

Today, 78 suppliers are accredited to provide services ranging from design - fab - mask manufacturing - packaging & testing.
78 Trusted Suppliers

As of 6 September 2017

Design         Aggregation         Broker         Mask Data Parsing            Mask Manufacturing            Foundry            Post-Processing            Packaging/Assembly            Test

ON Semiconductor Pocatello
Plexus Aerospace, Defense and Security Services
The Boeing Company
ON Semiconductor Gresham
Maxtek Components Corp.
TSI Semiconductors America
DMEA
Silicon Turnkey Solutions
Microsemi SOC San Jose
CORWIL Technology
Lockheed Martin SS Site
Atessa, Inc.
Pantronix Corp.
GDSI
e2v, Inc.
Six Sigma
DPA Components Int’l.
Raytheon Vision Systems
HRL Laboratories
USC-ISI Marina del Rey
USC-ISI MOSIS
Northrop Grumman AS
Boeing Network and Space Systems
Raytheon Space & Airborne Systems
Syphemia International
Arkham Technology Ltd.
Mercury System Phoenix Microelectronics Center
General Dynamics Mission Systems, Scottsdale
Raytheon Missile Systems
Silanna Semiconductor
L-3 Communications Systems
Integra Technologies
Lockheed Martin Space Systems, Denver Site
National Security Campus – Kansas City
Trusted Semiconductor Solutions Inc.
General Dynamics Mission Systems
Honeywell Aerospace Plymouth
SkyWater Technology Foundry
Rockwell Collins
Qorvo Texas, LLC
Criteria Labs, Inc.
TLMI
Novati Technologies, Inc.
Sandia National Laboratories MST&C
Aeroflex Colorado Springs

Northrop-Grumman Mission Systems
USG Microelectronic Solutions Group
JHU/APL
USC-ISI Arlington
BAE Systems Electronic Systems
CREE, Inc.
MacAulay-Brown, Inc.
Harris Corp. Government Communications Systems Division
Vortex Aerospace Design & Labs
Lockheed Martin Missiles and Fire Control, Orlando Site
Sypris Electronics
Aurora Semiconductor
Teledyne Microelectronic Technologies
The JFAC is a federation of DoD organizations that have a shared interest in promoting software and hardware assurance in defense acquisition programs, systems, and supporting activities. The JFAC member organizations and their technical service providers interact with program offices and other interested parties to provide software and hardware assurance expertise and support, to include vulnerability assessment, detection, analysis, and remediation services, and information about emerging threats and capabilities, software and hardware assessment tools and services, and best practices.

Source: DoD Joint Federated Assurance Center (JFAC) Industry Outreach, 2016 NDIA SE Conference, Tom Hurt, Distribution Statement A – Approved for public release by DOPSR. Case # 17-S-0032 applies. Distribution is unlimited, October 26, 2016
Joint Federated Assurance Center: Software and Hardware Assurance

• JFAC is a federation of DoD software and hardware assurance (SwA/HwA) capabilities and capacities to:
  – Provide SW and HW inspection, detection, analysis, risk assessment, and remediation tools and techniques to PM’s to mitigate risk of malicious insertion

• JFAC Coordination Center is developing SwA tool and license procurement strategy to provide:
  – Enterprise license agreements (ELAs) and ELA-like license packages for SwA tools used by all DoD programs and organizations
    • Initiative includes coordinating with NSA’s Center for Assured Software to address potential concerns about the security and integrity of the open source products
  – Automated license distribution and management system usable by every engineer in DoD and their direct-support contractors

• Lead DoD microelectronic hardware assurance capability providers
  – Naval Surface Warfare Center Crane
  – Army Aviation & Missile Research Development and Engineering Center
  – Air Force Research Lab

Moving Towards Full Operational Capability
JFAC Portal: https://jfac.army.mil/ (CAC-enabled)

Source: Engineering Cyber Resilient Weapon Systems, Kristen Baldwin, SAE Aerotech Congress, Cleared - Case # 17-S-1517, September 27, 2017
Microelectronics Trust Verification Technologies

- Verification needed when Trusted Foundry not available
  - DoD formed JFAC to provide this service
  - Long-term challenge to analyze leading-edge ICs and scale up capacity

Design Verification
- Verification/assurance of designs, IP, netlists, bit-streams, firmware, etc.

Physical Verification
- Destructive analysis of ICs and Printed Circuit Boards

Functional Verification
- Non-destructive screening and verification of select ICs

DoD, Intelligence Community, and DoE enhancing capability to meet future demand

Source: Long-Term Strategy for DoD Trusted and Assured Microelectronics Needs, Dr. Jeremy Muldavin, NDIA SE Conference, Distribution Statement A – Approved for public release by DOPSR, Case # 16-S-2895 applies. Distribution is unlimited, October, 26, 2017
Testing is unlikely to replace using a “Trustworthy” Supplier

- Lots purchase from “Trustworthy” source (such as OEM/Authorized Distributors) in active manufacture:
  - Quality at the 100-500 ppm level
  - Counterfeit rates are extremely rare, probably at levels nearing quality level
  - Acceptance testing adds nothing to the assurance of these lots
    - And the rate of false positives will mean much wasted effort analyzing good parts flagged as suspect
- Obsolete lots purchased from the independent market
  - Quality is likely to be in the range of 10,000 ppm
  - Still must test 300 parts to assure 10,000 ppm
  - Could never achieve quality of original authentic parts (100 ppm)
  - Low assurance will compromise reliability
  - Cost of testing (and handling false positives) could still add significantly to part cost
    - Advanced testing makes it even worse
- Impaired Sources – Possible bad handling, potential for counterfeit returns, etc.
  - Testing may do little to improve assurance
  - Rarity of defects may cause costs from false positives to outweigh any benefit from testing at all

On The Limits of Test in Establishing Products Assurance
Brian. S. Cohen and Kathy Lee, GOMACTech - 2014
Many ICs are Already Obsolete at Acquisition

- Counterfeits pose a serious acquisition issue
- Use of Obsolete High-Rel, High Temp ICs is readily targetable
- During sustainment substantial ICs will become obsolete

At Least 22% of ICs have Serious Obsolescence Risk

IC Use in 5 Major Systems Entering Production (Milestone C). A 2012 IDA study looked at Bills of Material for 5 current major defense acquisitions, characterizing the use of over 3000 unique ICs.
Forecasting Obsolescence

- Acquisition has a responsibility to manage life cycle SCRM risks related to DMSMS
  - Integrated circuit lifetimes can be short (12-18 months)
  - When a part becomes obsolete it may trigger major supply chain changes – buying from the aftermarket
- Programs can forecast DMSMS risks:
  - IHS – Commercial forecast from Bill of Materials (BOM)
  - OMIS – Navy system (currently assesses 50+ programs with 2.5 M parts)
- TSN Methodology Needs to Try to Predict Obsolescence Risk and Identify “Critical” components for the LifeCycle!

Source: IHS
Transition from Acquisition to Sustainment

Acquisition Process

- Service Engineering Support Activity (ESA) retains configuration control (Tech data)

Logistics Reassignment Process

- Governed by DoD 4140.26M (Vol 2 & 4)
- Service defines criticality of part
  - Critical Flight Safety
  - Critical Application
- Service defines Acquisition Strategy:
  - Sole source
  - Competitive bid

Sustainment Process

- Wholesale management of consumable items

Service Requirements

Integrated Materiel Management

10/31/2017
• Revised March 2017
  o Now includes procedures for managing and handling special trusted system network critical components (TSN CC)

• Defines Trusted System Network Critical Components (TSN CC) as a Controlled Inventory Item (CII)

• Procedures for maintaining inventory accountability, managing, handling of TSN CC
The DMSMS SCRM Conundrum

- Any Integrated Circuit (IC) will have a long-term likelihood of becoming obsolete - some more than others.
- The likelihood of an aftermarket IC being counterfeited is substantial (and highly targetable).
- Any IC that is deemed of “high consequence” is very likely to become a “red-red” sometime later in the life cycle.
- There are two ways of dealing with this:
  1. Any high consequence IC with forecasted obsolescence risk is considered a TSN critical component (TSN CC).
  2. All high consequence ICs are passed to sustainment at provisioning as a TSN CC but defers risk management decision is until encountered obsolescence raises a concern to an unacceptable level.
Acquisition Forecasts

• Acquisition programs should analyze BOM and Forecast Likelihood of Obsolescence
  
  o Use this as “Potential Risk”

• Advantages
  
  o This could leverage current policy and practice
  o Would enable acquisition program to proactively plan for DMSMS mitigation in order to manage critical SCRM IC program risks
  o Could be integrated into LCSP

• Disadvantages
  
  o A majority of ICs might be identified as potentially at risk
  o Poor long-term predictive capability for obsolescence
• SCRM is a risk management activity driven by the TSN analysis
  o Hardware Assurance (and Software Assurance) Assessments and Mitigations
  o Anti-Counterfeit Measures
  o Use of Trusted Suppliers

• New guidance helps connect acquisition to transfer “criticality” to sustainment
  o Driven by revision to DODM 4140.01 Volume 11
  o Defines TSN CC
  o Provides Structure for Sustainment to “prioritize” when obsolescence is a risk and how to reassess and mitigate risks
Backup Policy Details
The HwA Current Policy con’t

- **5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks**

  - Detect vulnerabilities within custom and commodity hardware and software through rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing.
  - In applicable systems, integrated circuit-related products and services shall be procured from a trusted supplier using trusted processes accredited by the Defense Microelectronics Activity (DMEA) when they are custom-designed, custom-manufactured, or tailored for a specific DoD military end use (generally referred to as application-specific integrated circuits (ASIC)).
  - **Definition: software assurance. The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle.**

  - In MSA: Identify system **(hardware and software) assurance** risks early to ensure system requirements, design, and architecture will produce a secure system in operations.

- **Section 937 of Public Law 113-66** Requires the DoD to establish a joint federation of capabilities to support trusted defense system needs to ensure the security of software and hardware developed, maintained, and used by the DoD.
The HwA Current Policy con’t

- **DOD 5000.02 Enclosure 14**, February 2, 2017
  - Use trusted suppliers or appropriate SCRM countermeasures for system elements that perform mission-critical functions. Cyber protection measures for mission-critical functions and critical components must, at a minimum, include **software assurance**, **hardware assurance**, procurement strategies, and anti-counterfeit practices in accordance with DoDI 5200.44
  - Request assistance, when appropriate, from the **Joint Federated Assurance Center**, established in accordance with Section 937 of Public Law 113-66, (Reference (j)) to support **software and hardware assurance** requirements
  - Incorporate cyber protection of program and system information, CPI, system elements (e.g., **hardware assurance and software assurance**) and cybersecurity performance requirements in the development RFP.