INSTITUTE FOR DEFENSE ANALYSES

Supply Chain Risk Management (SCRM)

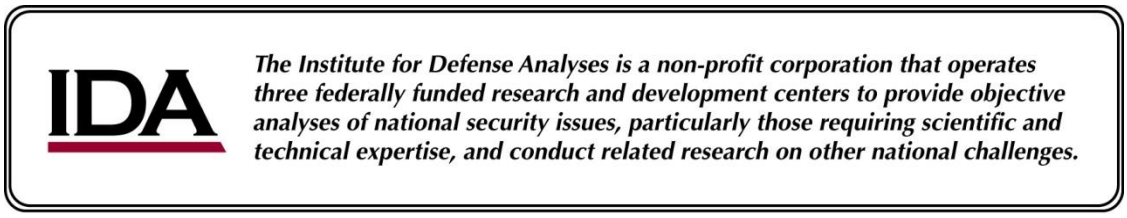
Brian S. Cohen

October 31, 2017

IDA Document
NS D-8876

INSTITUTE FOR DEFENSE
ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

Approved for public release; distribution is unlimited.



About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task AU-5-4302, "Trusted and Assured Microelectronics," for Deputy Assistant Secretary of Defense, Systems Engineering. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

For more information:

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

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Approved for public release; distribution is unlimited.

Institute for Defense Analyses
4850 Mark Center Drive • Alexandria, Virginia 22311-1882

Supply Chain Risk Management (SCRM)

Approved for public release; distribution is unlimited.

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

Recommendations from Defense Science Board

Summary of Recommendations

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

DSB TASK FORCE ON CYBER SUPPLY CHAIN 11

Approved for public release; distribution is unlimited.

Approved for public release; distribution is unlimited.

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

DoDM 5200.01, Vol. 1-4 | **DoDM 5200.45** | **DoDI 8500.01**

DoDI 5200.39 | **DoDI 5200.44** | **DoDI 5230.24** | **DoDI 8510.01**

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

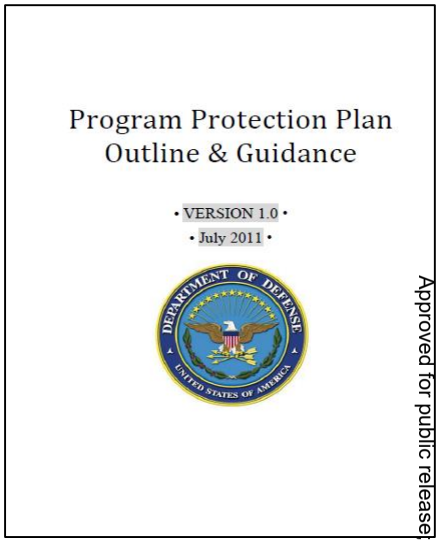
Approved for public release; distribution is unlimited.

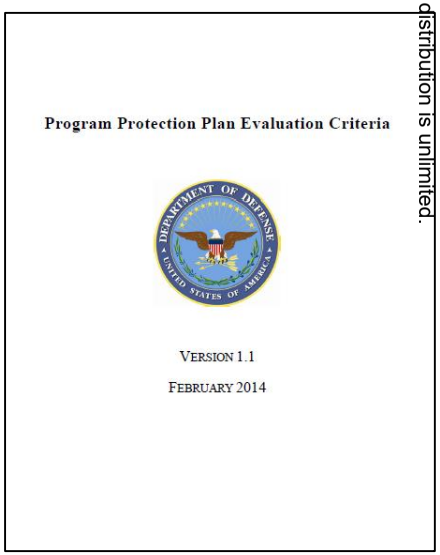
Policies, guidance and white papers are found at our initiatives site: http://www.acq.osd.mil/se/initiatives/init_pp-sse.html

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”
  - Programs have options on implementation
  - 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
Program Protection Plan Evaluation Criteria, Version 1.1, February 2014

Approved for public release; distribution is unlimited.

Why is LifeCycle SCRM Hard?

- Risk = Function (Threat, Vulnerability, Consequence)
  - Consequence – How Serious Is Impact On System/Mission?
  - Vulnerability – How Readily Will A Component Compromise Cause A Consequence
  - Criticality = Function (Consequence And Vulnerability)
  - Threat – Adversary Motivation, Capability And Access
  - 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)

Approved for public release; distribution is unlimited.

Program Protection Integrated into Policy

IDA

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

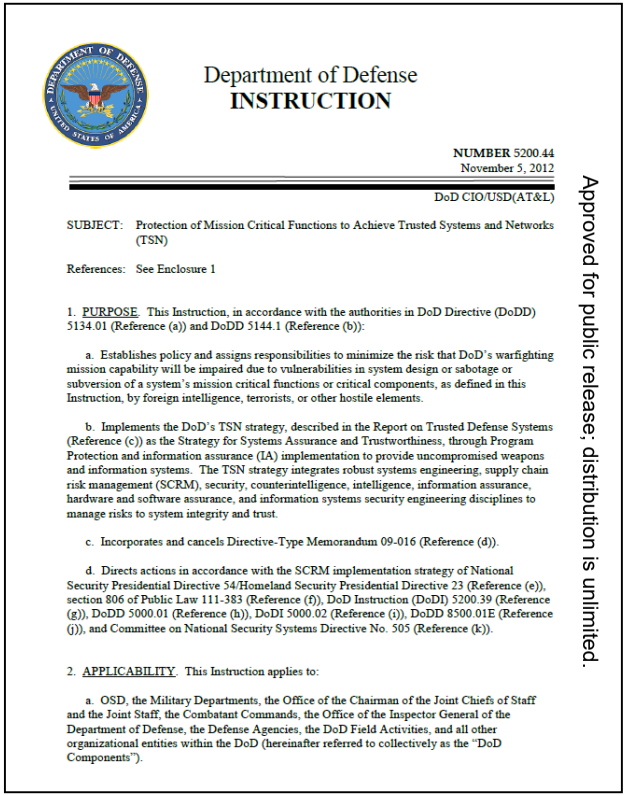
SCRM Policy is In RED

Approved for public release; distribution is unlimited.

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 - Trusted Systems and Network (TSN) Policy

- 5200.44 Defines the Supply Chain Risk Management (SCRM) Policy
- What does it say about Microelectronics? (Policy Section 4)
  - 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
  - E. …Custom integrated circuit-related products and services shall be procured from a trusted supply chain



Department of Defense
INSTRUCTION

NUMBER 5200.44
November 5, 2012

DoD CIO/USD(AT&L)

SUBJECT: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

References: See Enclosure 1

1. PURPOSE. This Instruction, in accordance with the authorities in DoD Directive (DoDD) 5134.01 (Reference (a)) and DoDD 5144.1 (Reference (b)):

a. Establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components, as defined in this Instruction, by foreign intelligence, terrorists, or other hostile elements.

b. Implements the DoD's TSN strategy, described in the Report on Trusted Defense Systems (Reference (c)) as the Strategy for Systems Assurance and Trustworthiness, through Program Protection and information assurance (IA) implementation to provide uncompromised weapons and information systems. The TSN strategy integrates robust systems engineering, supply chain risk management (SCRM), security, counterintelligence, intelligence, information assurance, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust.

c. Incorporates and cancels Directive-Type Memorandum 09-016 (Reference (d)).

d. Directs actions in accordance with the SCRM implementation strategy of National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (e)), section 806 of Public Law 111-383 (Reference (f)), DoD Instruction (DoDI) 5200.39 (Reference (g)), DoDD 5000.01 (Reference (h)), DoDI 5000.02 (Reference (i)), DoDD 8500.01E (Reference (j)), and Committee on National Security Systems Directive No. 505 (Reference (k)).

2. APPLICABILITY. This Instruction applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

Approved for public release; distribution is unlimited.

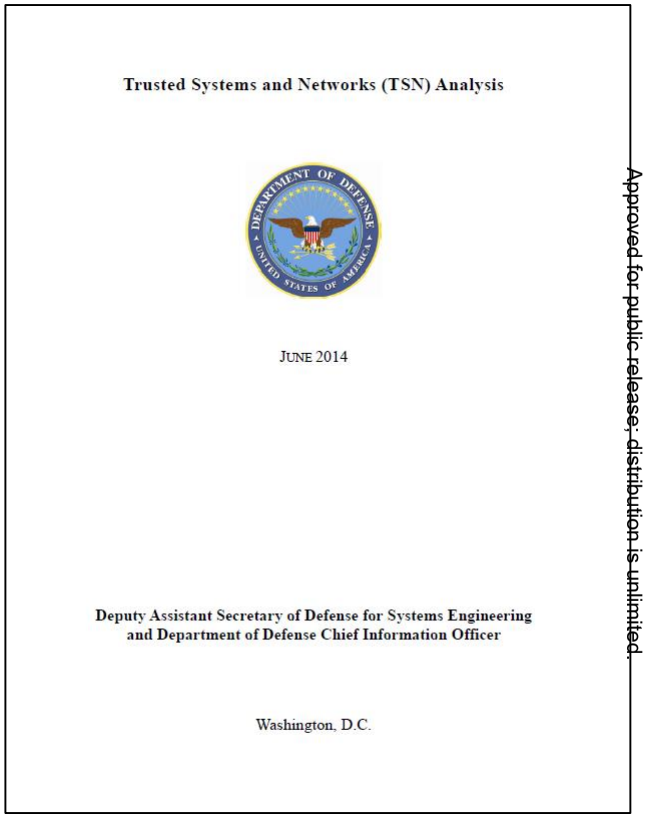
Issued November 5, 2012
Last Change July 27, 2017

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

Approved for public release; distribution is unlimited.

How to Implement Policy

- All depend on TSN Risk Analysis
- Assessment and Mitigations Are in Three "Lanes"
  - Anti-Counterfeit Measures
  - Use of Trusted Suppliers for ASICs
  - Hardware and Software Assurance (HwA and SwA) – including the use of the Joint Federated Assurance Centers (JFAC)
- Anti-Counterfeit
  - Use Original Component Manufacturer Authorized Distributor, Use Counterfeit Screening (i.e. AS5553) if possible


Trusted Systems and Networks (TSN) Analysis

JUNE 2014

Deputy Assistant Secretary of Defense for Systems Engineering
and Department of Defense Chief Information Officer

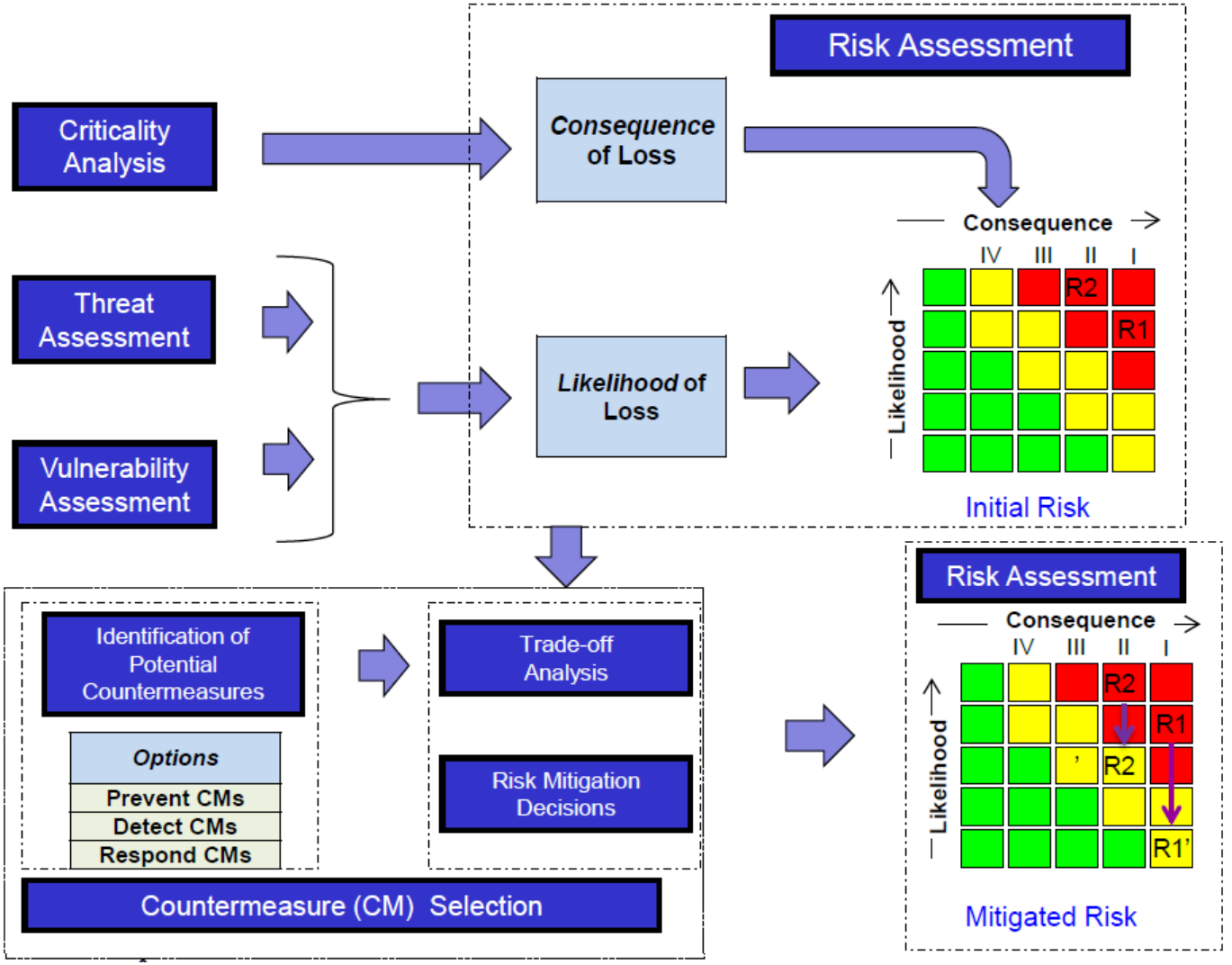
Washington, D.C.

Trusted Systems and Networks (TSN) Analysis, June 2014

Additional Guidance in the Defense Acquisition Guidebook (DAG Chapter 9) - Program Protection (PDF Version)

Approved for public release; distribution is unlimited.

TSN Methodology



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

Approved for public release; distribution is unlimited.

Trusted Foundry Program Created to Mitigate Risks

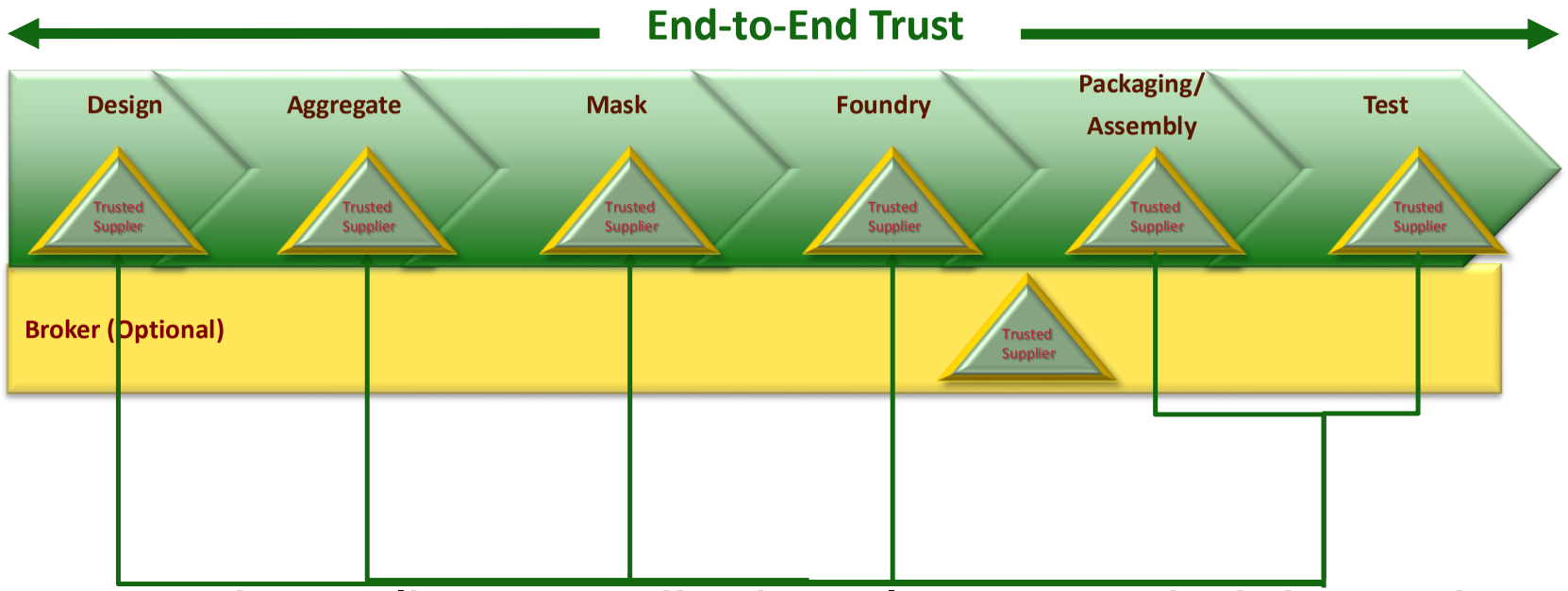
IDA

- 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

Approved for public release; distribution is unlimited.

A Trusted Supply Chain

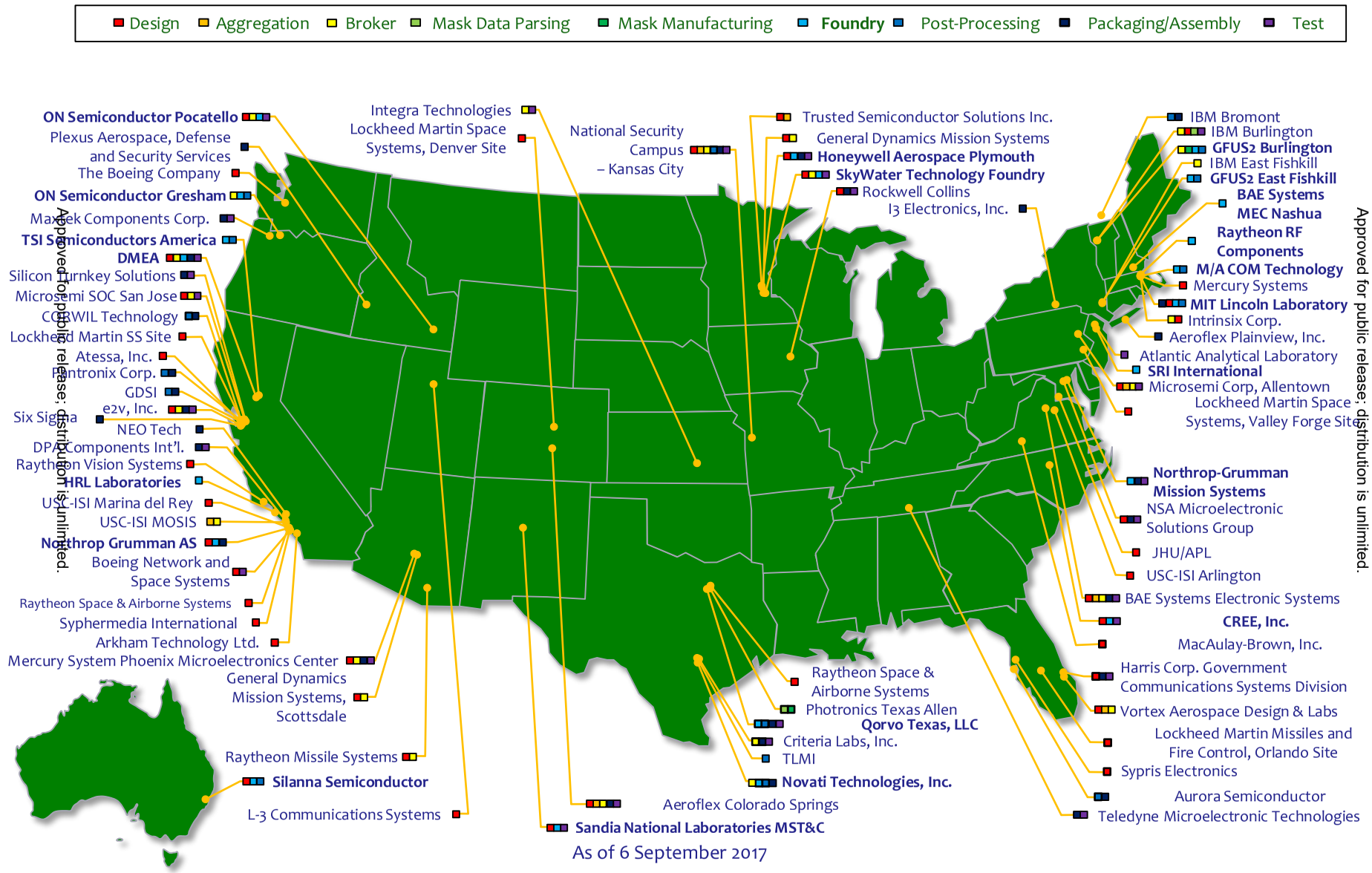


- Trusted supplier accreditation plan expanded the ranks of suppliers capable of providing trusted services for leading-edge, state-of-the-practice and legacy parts by certifying that suppliers meet a comprehensive set of security and operations criteria

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

Approved for public release; distribution is unlimited.

78 Trusted Suppliers



JFAC Mission

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

Approved for public release; distribution is unlimited.

Joint Federated Assurance Center: Software and Hardware Assurance

IDA

- **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

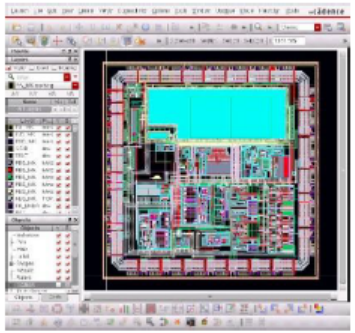
Approved for public release; distribution is unlimited.

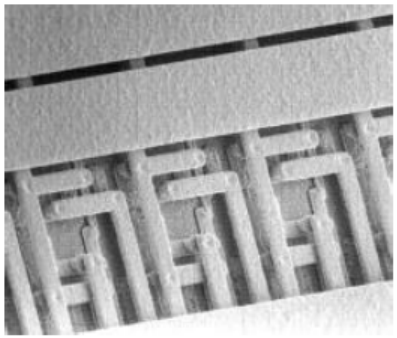
Microelectronics Trust Verification Technologies

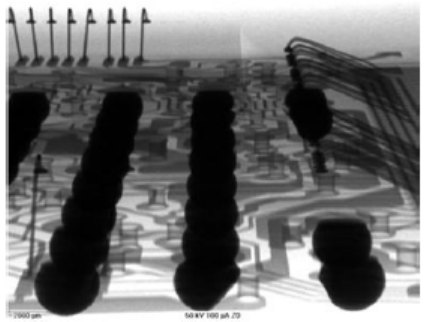
IDA

- **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	Physical Verification	Functional Verification
• Verification/assurance of designs, IP, netlists, bit-streams, firmware, etc.	• Destructive analysis of ICs and Printed Circuit Boards	• Non-destructive screening and verification of select ICs







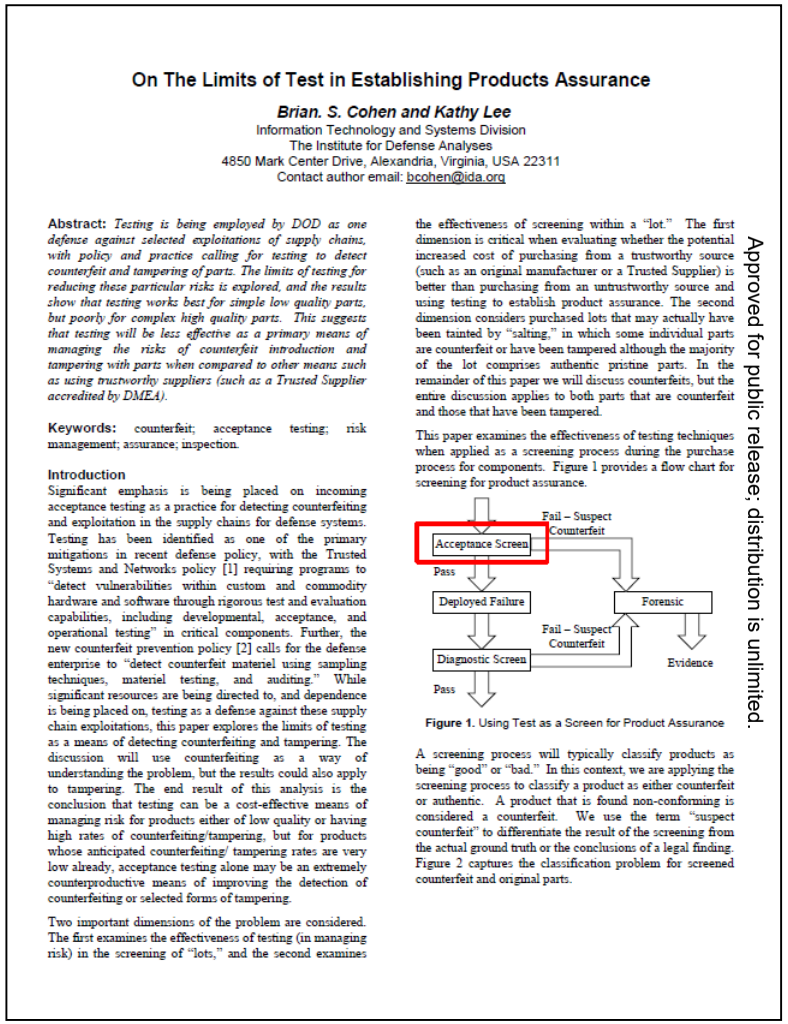
Approved for public release; distribution is unlimited.

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
Information Technology and Systems Division
The Institute for Defense Analyses
4850 Mark Center Drive, Alexandria, Virginia, USA 22311
Contact author email: bcohen@ida.org

Abstract: *Testing is being employed by DOD as one defense against selected exploitations of supply chains, with policy and practice calling for testing to detect counterfeit and tampering of parts. The limits of testing for reducing these particular risks is explored, and the results show that testing works best for simple low quality parts, but poorly for complex high quality parts. This suggests that testing will be less effective as a primary means of managing the risks of counterfeit introduction and tampering with parts when compared to other means such as using trustworthy suppliers (such as a Trusted Supplier accredited by DMEA).*

Keywords: counterfeit; acceptance testing; risk management; assurance; inspection.

Introduction

Significant emphasis is being placed on incoming acceptance testing as a practice for detecting counterfeiting and exploitation in the supply chains for defense systems. Testing has been identified as one of the primary mitigations in recent defense policy, with the Trusted Systems and Networks policy [1] requiring programs to "detect vulnerabilities within custom and commodity hardware and software through rigorous test and evaluation capabilities, including developmental, acceptance, and operational testing" in critical components. Further, the new counterfeit prevention policy [2] calls for the defense enterprise to "detect counterfeit materiel using sampling techniques, materiel testing, and auditing." While significant resources are being directed to, and dependence is being placed on, testing as a defense against these supply chain exploitations, this paper explores the limits of testing as a means of detecting counterfeiting and tampering. The discussion will use counterfeiting as a way of understanding the problem, but the results could also apply to tampering. The end result of this analysis is the conclusion that testing can be a cost-effective means of managing risk for products either of low quality or having high rates of counterfeiting/tampering, but for products whose anticipated counterfeiting/ tampering rates are very low already, acceptance testing alone may be an extremely counterproductive means of improving the detection of counterfeiting or selected forms of tampering.

Two important dimensions of the problem are considered. The first examines the effectiveness of testing (in managing risk) in the screening of "lots," and the second examines the effectiveness of screening within a "lot." The first dimension is critical when evaluating whether the potential increased cost of purchasing from a trustworthy source (such as an original manufacturer or a Trusted Supplier) is better than purchasing from an untrustworthy source and using testing to establish product assurance. The second dimension considers purchased lots that may actually have been tainted by "salting," in which some individual parts are counterfeit or have been tampered although the majority of the lot comprises authentic pristine parts. In the remainder of this paper we will discuss counterfeits, but the entire discussion applies to both parts that are counterfeit and those that have been tampered.

This paper examines the effectiveness of testing techniques when applied as a screening process during the purchase process for components. Figure 1 provides a flow chart for screening for product assurance.

Figure 1. Using Test as a Screen for Product Assurance

A screening process will typically classify products as being "good" or "bad." In this context, we are applying the screening process to classify a product as either counterfeit or authentic. A product that is found non-conforming is considered a counterfeit. We use the term "suspect counterfeit" to differentiate the result of the screening from the actual ground truth or the conclusions of a legal finding. Figure 2 captures the classification problem for screened counterfeit and original parts.

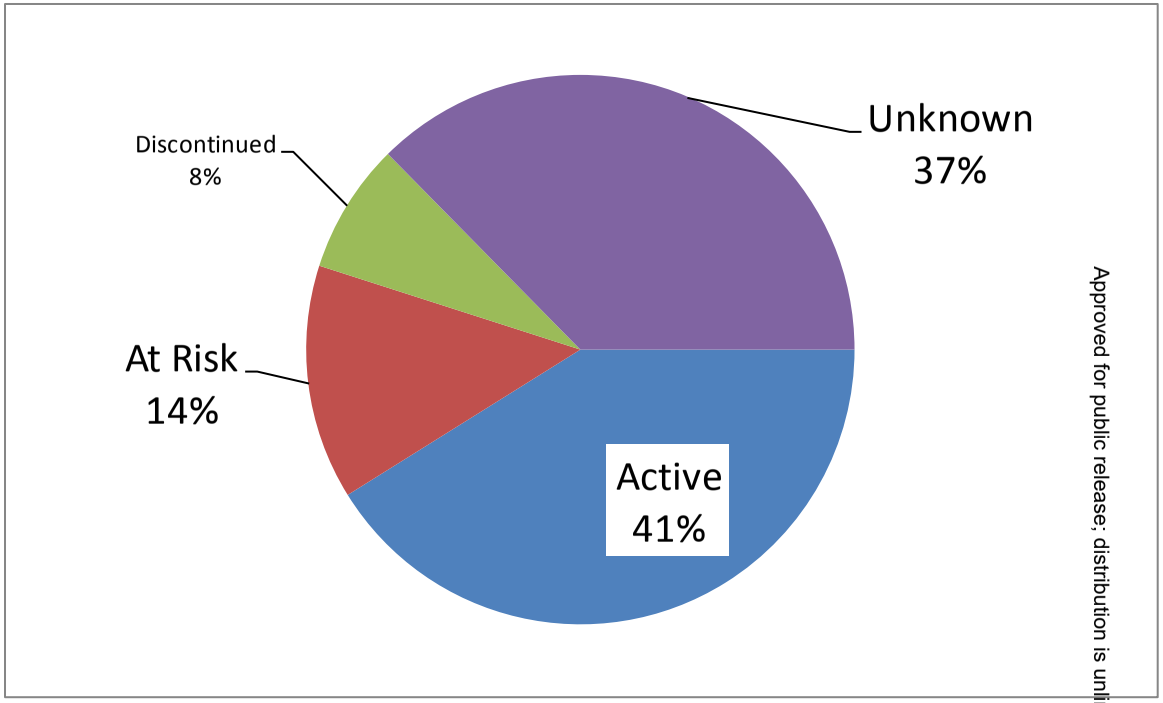
On The Limits of Test in Establishing Products Assurance
Brian. S. Cohen and Kathy Lee, GOMACTech - 2014

Approved for public release; distribution is unlimited.

Many ICs are Already Obsolete at Acquisition

IDA

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



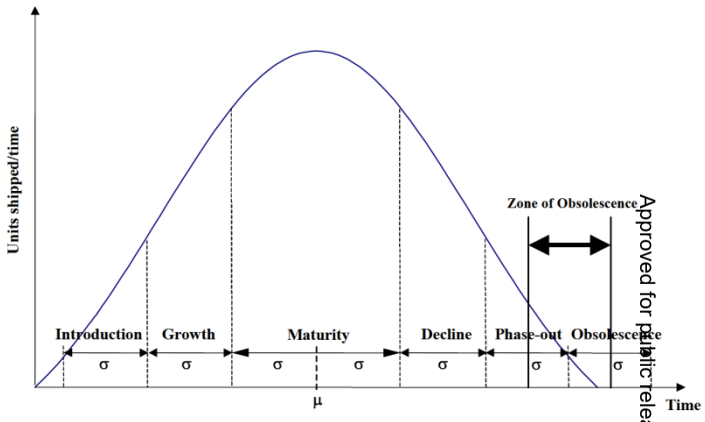
At Least 22% of ICs have Serious Obsolescence Risk

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

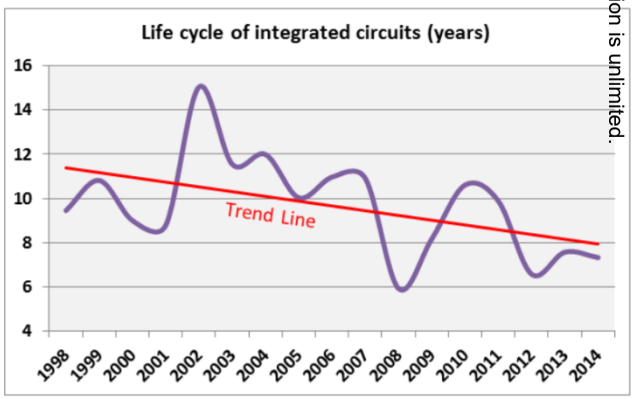
Approved for public release; distribution is unlimited.

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!



IEEE Trans. on Components and Packaging Technologies, Dec. 2000, pp. 707-717, Solomon, et al



Source IHS

Approved for public release; distribution is unlimited.

Transition from Acquisition to Sustainment

IDA

Acquisition Process

Logistics Reassignment Process

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

Sustainment Process

Approved for public release; distribution is unlimited.

Approved for public release; distribution is unlimited.

Service Requirements

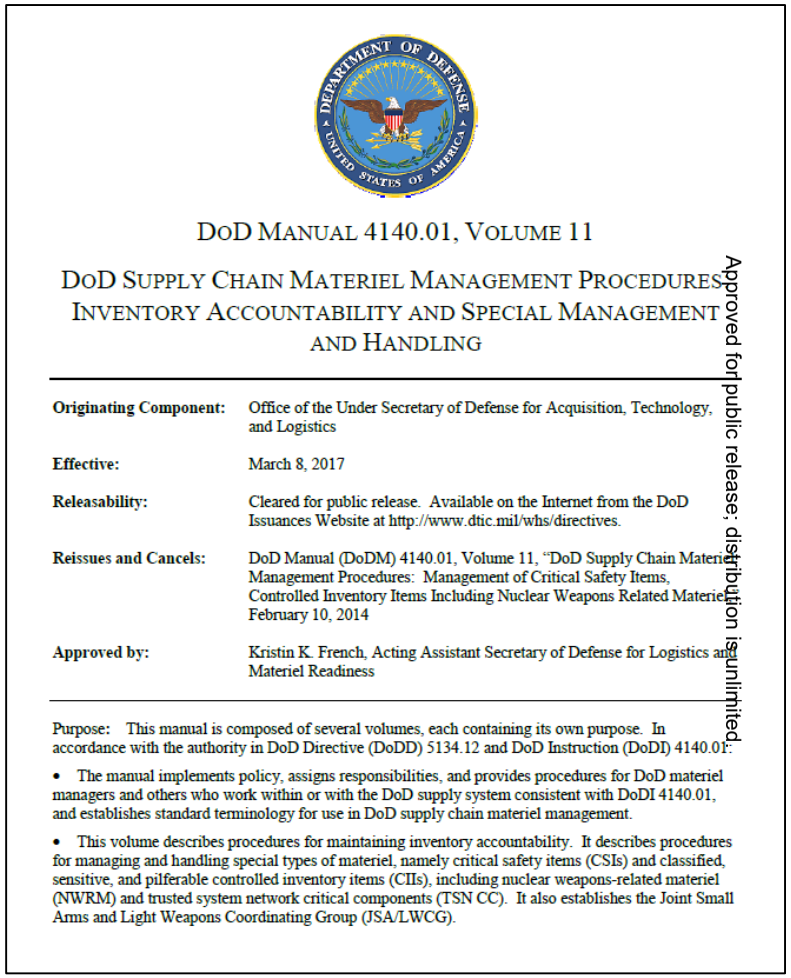
Integrated Materiel Management

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

Wholesale management of consumable items

DoDM 4140.01 Vol 11 Revised

- Revised March 2017
  - 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



DoD Manual 4140.01, Volume 11

DoD Supply Chain Materiel Management Procedures: Inventory Accountability and Special Management and Handling

Originating Component:	Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics
Effective:	March 8, 2017
Releasability:	Cleared for public release. Available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.
Reissues and Cancels:	DoD Manual (DoDM) 4140.01, Volume 11, "DoD Supply Chain Materiel Management Procedures: Management of Critical Safety Items, Controlled Inventory Items Including Nuclear Weapons Related Materiel," February 10, 2014
Approved by:	Kristin K. French, Acting Assistant Secretary of Defense for Logistics and Materiel Readiness

Purpose: This manual is composed of several volumes, each containing its own purpose. In accordance with the authority in DoD Directive (DoDD) 5134.12 and DoD Instruction (DoDI) 4140.01:

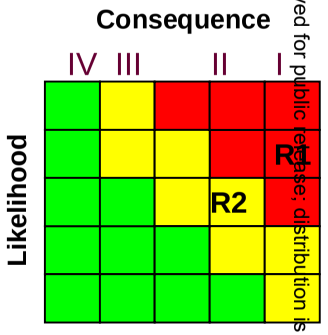
- The manual implements policy, assigns responsibilities, and provides procedures for DoD materiel managers and others who work within or with the DoD supply system consistent with DoDI 4140.01, and establishes standard terminology for use in DoD supply chain materiel management.
- This volume describes procedures for maintaining inventory accountability. It describes procedures for managing and handling special types of materiel, namely critical safety items (CSIs) and classified, sensitive, and pilferable controlled inventory items (CIIs), including nuclear weapons-related materiel (NWRM) and trusted system network critical components (TSN CC). It also establishes the Joint Small Arms and Light Weapons Coordinating Group (JSA/LWCG).

Approved for public release; distribution is unlimited.

DODM 4140.01 Volume 11, DoD Supply Chain Materiel Management Procedures: Inventory Accountability And Special Management And Handling, Revised March 8, 2017

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



Approved for public release; distribution is unlimited.

Acquisition Forecasts

- Acquisition programs should analyze BOM and Forecast Likelihood of Obsolescence
  - Use this as “Potential Risk”
- Advantages
  - This could leverage current policy and practice
  - Would enable acquisition program to proactively plan for DMSMS mitigation in order to manage critical SCRM IC program risks
  - Could be integrated into LCSP
- Disadvantages
  - A majority of ICs might be identified as potentially at risk
  - Poor long-term predictive capability for obsolescence

Approved for public release; distribution is unlimited.

Summary

- SCRM is a risk management activity driven by the TSN analysis
  - Hardware Assurance (and Software Assurance) Assessments and Mitigations
  - Anti-Counterfeit Measures
  - Use of Trusted Suppliers
- New guidance helps connect acquisition to transfer "criticality" to sustainment
  - Driven by revision to DODM 4140.01 Volume 11
  - Defines TSN CC
  - Provides Structure for Sustainment to "prioritize" when obsolescence is a risk and how to reassess and mitigate risks

Approved for public release; distribution is unlimited.

Institute for Defense Analyses
4850 Mark Center Drive • Alexandria, Virginia 22311-1882

Backup
Policy Details

Approved for public release; distribution is unlimited.

The HwA Current Policy cont'd

- 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks
- (TSN) (Aug 25, 2016)
  - *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.***
- DOD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs (Jan 2017)
  - *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*

Approved for public release; distribution is unlimited.

The HwA Current Policy

- DOD 5000.02 Enclosure 14, February 2, 2017
  - *ACTIVITIES TO MITIGATE CYBERSECURITY RISKS. Program Managers will rely on existing cybersecurity standards tailored to reflect analysis of specific program risks and opportunities to determine the level of cyber protections needed for their program information, the system, enabling and support systems, and information types that reside in or transit the fielded system. Appropriate cyber threat protection measures include information safeguarding, designed in system protections,* ***supply chain risk management (SCRM), software assurance, hardware assurance, anti-counterfeit practices, anti-tamper (AT)****, and program security related activities such as information security, operations security (OPSEC), personnel security, physical security, and industrial security.*

Current Policy and Guidance and other resources are available on the DASD(SE) website at http://www.acq.osd.mil/se/pg/index.html.

Approved for public release; distribution is unlimited.

The HwA Current Policy cont'd

- 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.*

Approved for public release; distribution is unlimited.

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
31-10-17	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Supply Chain Risk Management (SCRM)	HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Brian S. Cohen	AU-5-4302
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	NS D-8876

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Dr. Jeremy Muldavin Deputy Assistant Secretary of Defense, Systems Engineering 4800 Mark Center Drive Suite E16E08 Alexandria, VA 22350-3600	AU/DASD, SE
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Brian S. Cohen

14. ABSTRACT

Supply Chain Risk Management (SCRM) is a risk management process that supports the protection of systems across the life cycle against malicious threats. These threats range from nation state to criminal malicious actions. This presentation describes the strategy, policy and guidance for SCRM with a particular emphasis on the life cycle. This presentation highlights the connection between acquisition and sustainment and the processes that are used to connect the SCRM activities across those activities.

15. SUBJECT TERMS

Supply Chain Risk Management (SCRM)

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Jeremy Muldavin
Unclassified	Unclassified	Unclassified	Unlimited	27	19b. TELEPHONE NUMBER (Include Area Code) (571) 372-6690

Approved for public release; distribution is unlimited.

Approved for public release; distribution is unlimited.