Missile Defense Agency Small Business Conference
Supply Chain Risk Management (SCRM)
Information Briefing

Mr. David S. Lane
Assistant Director
BMDS Acquisition Security
Missile Defense Agency
13-14 August 2015

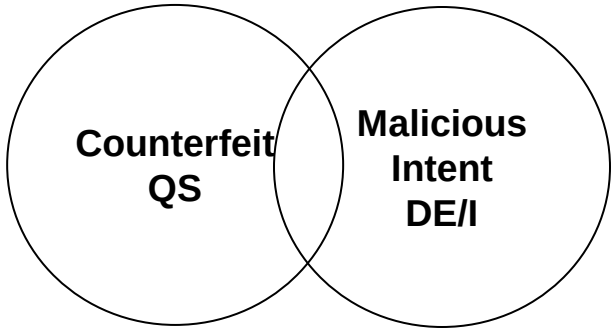
Agenda

- Purpose
- Bottom Line Upfront
- OSD and MDA Policy and Guidance
- “World is Flat”
- What are we protecting?
- SCRM Statement Of Work (SOW) Example
- Risks and SCRM Advisory
- Program Protection Lifecycle
- Software/Software Assurance vs. Info Assurance
- SCRAP vs. DEMILITARIZATION
- OSD Joint Federated Assurance Center (JFAC)

Purpose

Inform and update about current MDA implementation of Supply Chain Risk Management (SCRM)

- **Review what MDA is doing to guard against the introduction of parts with malicious intent by a foreign adversary to disrupt, disable, or render ineffective BMDS systems.***



SCRM

*** Separate from risk of substandard counterfeited parts which is also of concern and the focus of established QS activities.**

Approved for Public Release
15-MDA-8354 (12 August 15)

Bottom Line Up Front

- **It is a DoD requirement for all national security systems to conduct a Critical Program Information (CPI) Assessment and a Criticality Analysis**
  - **Our adversaries continue to target our technologies in an attempt to kill, counter, copy or clone our capabilities**
  - **Many BMDS contractors procure parts from foreign sources because of cost and availability considerations, which exposes the our system to a degree of risk that is difficult to define and mitigate.**
  - **MDA is building a weapons system utilizing parts procured from the same foreign sources that we are trying to defend against. - DoD CIO**

SCRM Requirement

DoD components will, by September 1, 2012, implement initial operating capability (IOC) of SCRM key practices within Information and Communications Technology (ICT) commodity purchase, systems acquisition and test and evaluation processes to mitigate supply chain risks to mission critical systems. Components will ensure by September 1, 2014 full operating capability (FOC) performance of trusted defense systems strategy for SCRM, in compliance with DTM 08-048, DoD 5200.39, and other applicable SCRM policy.

FY 12 Defense Planning and Programming Guidance, Para 6.5

Note: DoD has subsequently published DoDI 5200.44 to implement SCRM Policy

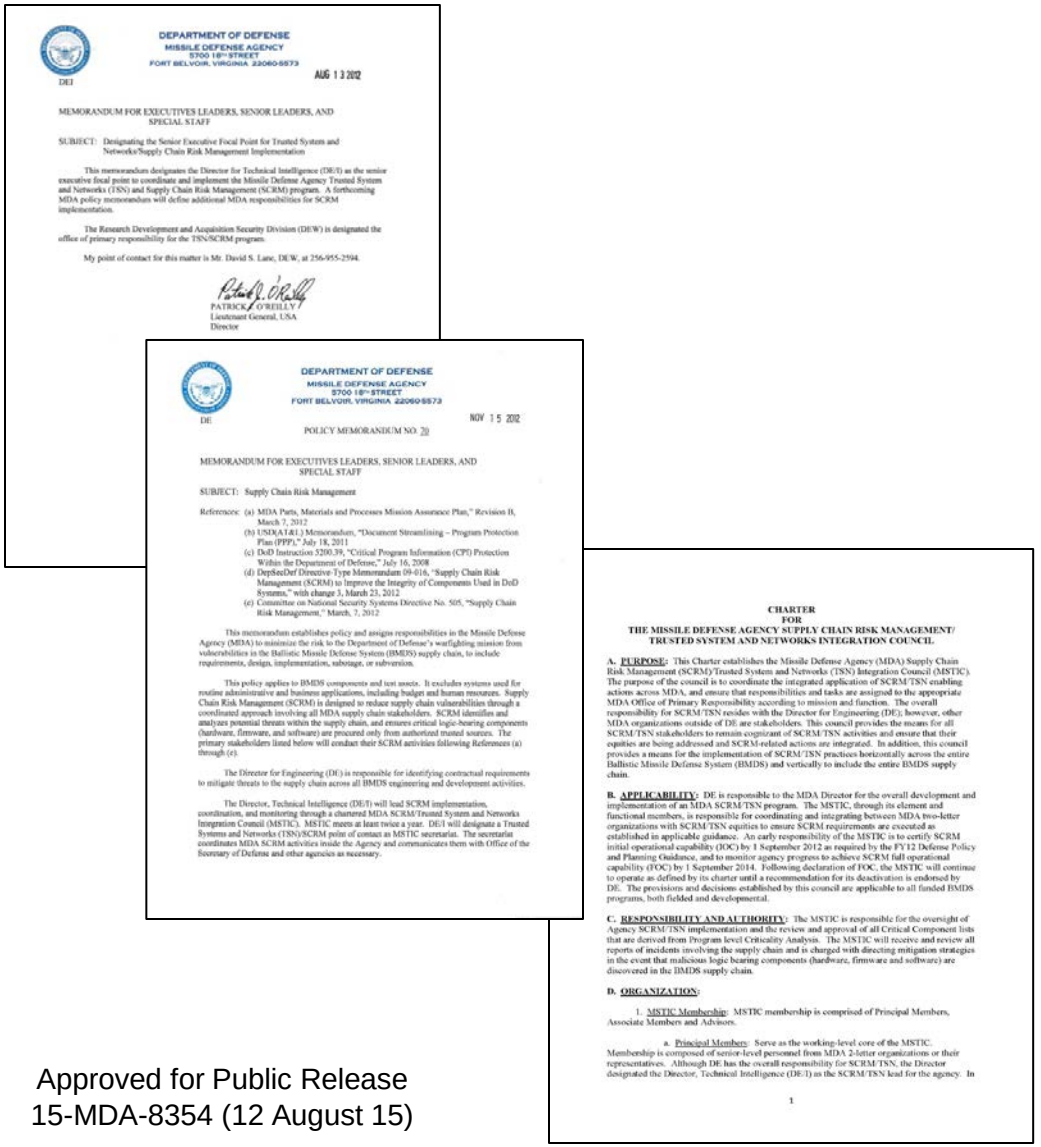
SCRM Problem Statement

Vulnerabilities in supply chain could lead to malicious logic insertions

- **Current DoD-unique Applied Specific Integrated Circuits (ASICs) used in DoD systems are procured via a Trusted Supplier chain per DoD policy**
  - Accounts for approximately 10% of logic-bearing DoD Integrated Circuit (IC) products used in DoD systems
- **Approximately 72% of DoD MicroE are non-ASICs; largely Field Programmable Gate Array (FPGA) devices**
  - DoD has no current trusted supply chain for FPGAs
  - FPGAs include COTS and Military grade products
  - Much of the FPGA value chain is off-shore, e.g., design, fabrication, programming services, testing and packaging
- **FPGAs that are programmed by DoD end-users may face Software Assurance (SwA) risks in FPGA bitstream programming tools, environment, and processes**
- **Bottom line: ASICs & FPGAs are not the only MicroE of concern (must address more than ASIC foundry operations)**

MDA Policy

- **MDA Director designated DE as the Executive Level SCRM Focal Point/Agency POC and DE/I as Executive Lead for SCRM planning and implementation**
  - **RDA Security and Counterintelligence (CI) reps began attending monthly OSD SCRM Roundtable meetings**
- **MDA Director approved Agency SCRM Policy**
- **Established an Agency Executive Level SCRM Integration Council (Chaired by DE/I)**



DEPARTMENT OF DEFENSE
MISSILE DEFENSE AGENCY
5700 18TH STREET
FORT BELVOIR, VIRGINIA 22060-5573

AUG 13 2012

MEMORANDUM FOR EXECUTIVES LEADERS, SENIOR LEADERS, AND SPECIAL STAFF

SUBJECT: Designating the Senior Executive Focal Point for Trusted System and Networks/Supply Chain Risk Management Implementation

This memorandum designates the Director for Technical Intelligence (DE/I) as the senior executive focal point to coordinate and implement the Missile Defense Agency Trusted System and Networks (TSN) and Supply Chain Risk Management (SCRM) program. A forthcoming MDA policy memorandum will define additional MDA responsibilities for SCRM implementation.

The Research Development and Acquisition Security Division (DEW) is designated the office of primary responsibility for the TSN/SCRM program.

My point of contact for this matter is Mr. David S. Lane, DEW, at 256-955-2594.

PATRICK O'REILLY
Lieutenant General, USA
Director

DEPARTMENT OF DEFENSE
MISSILE DEFENSE AGENCY
5700 18TH STREET
FORT BELVOIR, VIRGINIA 22060-5573

NOV 15 2012

POLICY MEMORANDUM NO. 20

MEMORANDUM FOR EXECUTIVES LEADERS, SENIOR LEADERS, AND SPECIAL STAFF

SUBJECT: Supply Chain Risk Management

References: (a) MDA Parts, Materials and Processes Mission Assurance Plan," Revision B, March 7, 2012
(b) USD(AT&L) Memorandum, "Document Streamlining – Program Protection Plan (PPP)," July 18, 2011
(c) DoD Instruction 5200.39, "Critical Program Information (CPI) Protection Within the Department of Defense," July 16, 2008
(d) DepSecDef Directive Type Memorandum 09-016, "Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems," with change 3, March 23, 2012
(e) Committee on National Security Systems Directive No. 505, "Supply Chain Risk Management," March, 7, 2012

This memorandum establishes policy and assigns responsibilities in the Missile Defense Agency (MDA) to minimize the risk to the Department of Defense's warfighting mission from vulnerabilities in the Ballistic Missile Defense System (BMDS) supply chain, to include requirements, design, implementation, sabotage, or subversion.

This policy applies to BMDS components and test assets. It excludes systems used for routine administrative and business applications, including budget and human resources. Supply Chain Risk Management (SCRM) is designed to reduce supply chain vulnerabilities through a coordinated approach involving all MDA supply chain stakeholders. SCRM identifies and analyzes potential threats within the supply chain, and ensures critical logic-bearing components (hardware, firmware, and software) are procured only from authorized trusted sources. The primary stakeholders listed below will conduct their SCRM activities following References (a) through (e).

The Director for Engineering (DE) is responsible for identifying contractual requirements to mitigate threats to the supply chain across all BMDS engineering and development activities.

The Director, Technical Intelligence (DE/I) will lead SCRM implementation, coordination, and monitoring through a chartered MDA SCRM/Trusted System and Networks Integration Council (MSTIC). MSTIC meets at least twice a year. DE/I will designate a Trusted Systems and Networks (TSN)/SCRM point of contact as MSTIC secretariat. The secretariat coordinates MDA SCRM activities inside the Agency and communicates them with Office of the Secretary of Defense and other agencies as necessary.

CHARTER
FOR
THE MISSILE DEFENSE AGENCY SUPPLY CHAIN RISK MANAGEMENT/ TRUSTED SYSTEM AND NETWORKS INTEGRATION COUNCIL

A. PURPOSE: This Charter establishes the Missile Defense Agency (MDA) Supply Chain Risk Management (SCRM)/Trusted System and Networks (TSN) Integration Council (MSTIC). The purpose of the council is to coordinate the integrated application of SCRM/TSN enabling actions across MDA, and ensure that responsibilities and tasks are assigned to the appropriate MDA Office of Primary Responsibility according to mission and function. The overall responsibility for SCRM/TSN resides with the Director for Engineering (DE); however, other MDA organizations outside of DE are stakeholders. This council provides the means for all SCRM/TSN stakeholders to remain cognizant of SCRM/TSN activities and ensure that their equities are being addressed and SCRM-related actions are integrated. In addition, this council provides a means for the implementation of SCRM/TSN practices horizontally across the entire Ballistic Missile Defense System (BMDS) and vertically to include the entire BMDS supply chain.

B. APPLICABILITY: DE is responsible to the MDA Director for the overall development and implementation of an MDA SCRM/TSN program. The MSTIC, through its element and functional members, is responsible for coordinating and integrating between MDA two-letter organizations with SCRM/TSN equities to ensure SCRM requirements are executed as established in applicable guidance. An early responsibility of the MSTIC is to certify SCRM initial operational capability (IOC) by 1 September 2012 as required by the FY12 Defense Policy and Planning Guidance, and to monitor agency progress to achieve SCRM full operational capability (FOC) by 1 September 2014. Following declaration of FOC, the MSTIC will continue to operate as defined by its charter until a recommendation for its deactivation is endorsed by DE. The provisions and decisions established by this council are applicable to all funded BMDS programs, both fielded and developmental.

C. RESPONSIBILITY AND AUTHORITY: The MSTIC is responsible for the oversight of Agency SCRM/TSN implementation and the review and approval of all Critical Component lists that are derived from Program level Criticality Analysis. The MSTIC will receive and review all reports of incidents involving the supply chain and is charged with directing mitigation strategies in the event that malicious logic bearing components (hardware, firmware and software) are discovered in the BMDS supply chain.

D. ORGANIZATION:

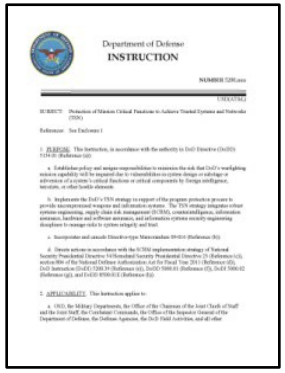
1. MSTIC Membership: MSTIC membership is comprised of Principal Members, Associate Members and Advisors.

a. Principal Members: Serve as the working-level core of the MSTIC. Membership is composed of senior-level personnel from MDA 2-letter organizations or their representatives. Although DE has the overall responsibility for SCRM/TSN, the Director designated the Director, Technical Intelligence (DE/I) as the SCRM/TSN lead for the agency. In

1

Approved for Public Release
15-MDA-8354 (12 August 15)

Program Protection Integrated Supply Chain Policy


Department of Defense
INSTRUCTION

DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

- Requires AT&L to develop a strategy for managing risk in the supply chain for integrated circuit-related products and services (e.g., FPGAs, printed circuit boards) that are identifiable to the supplier as specifically created or modified for DoD (e.g., military temperature range, radiation hardened).


DEPARTMENT OF DEFENSE

DoD
Supply Chain Materiel
Management Regulation

MAY 25, 2003

Office of the Deputy Under Secretary of Defense for
Logistics and Materiel Readiness

DoD 4140.1-R, DoD Supply Chain Materiel Management Regulation

- Requires quality assurance methods including contractor selection and qualification programs; quality requirements; pre-award surveys; Government inspection; and testing.
- Quality assurance techniques and testing should stress conforming CAI to contract and technical requirements.

Proposition: Add security risk criteria to safety, reliability, etc. for Critical Application Items (CAI) designation in the supply chain to assist in managing MicroE CCs throughout the lifecycle

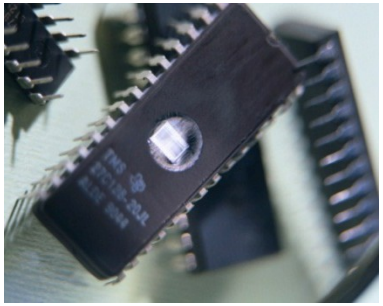
DoD Issuances Website: http://www.dtic.mil/whs/directives/corres/ins1.html

Trusted Defense Systems Strategy
Basic Tenets

- **Prioritization:**
  - Focus security requirements on mission critical systems
  - Within systems, identify and protect critical components, technology, information
- **Comprehensive Program Protection Planning**
  - Early lifecycle identification of critical components
  - Provide Program Managers with analysis of supply chain risk
  - Protect critical components through trusted suppliers, or secure systems design
  - Assure systems through advanced vulnerability detection, test and evaluation
- **Partner with Industry**
  - Develop commercial standards for secure products
- **Enhance capability through Research and Development**
  - Leverage and enhance vulnerability detection tools and capabilities
  - Technology investment to advance secure software, hardware, and system design methods

Proposition: Trust Policy Objective

- **Implement Supply Chain Risk Management (SCRM) on MicroE components used in National Security Systems when military end use is identifiable - thus targetable for malicious acts; in particular, when:**
  - Used in intelligence, crypto, command & control, and weapon systems,
  - Critical to military or intelligence mission success, or
  - They manage classified information
- **MicroE component attributes of interest include, but are not limited to:**
  - Defining a sequence of instructions,
  - Performing one or more decision making functions,
  - Executing basic units of logic,
  - Or, can be altered surreptitiously to trigger malicious functionality or the loss of confidential information.



- **Examples of MicroE that may be critical include vulnerable custom ASICs, programmable logic devices (e.g., FPGAs), micro-processors, Application Specific Standard Products, and flash memories**

How do we find them and mitigate the risk?

FY 11 National Defense Authorization Act, Section 806

- **Section 806 for FY 2011 National Defense Authorization Act (NDAA) permits consideration of supply chain risk in a source selection or consideration of proposals for a task/delivery order related to a National Security System (NSS) using three approaches:**
  - **SCRM evaluation factors: head of agency may exclude an offeror who fails to achieve an acceptable rating on a supply chain risk evaluation factor**
  - **Limitations on subcontracting: head of an agency may withhold consent to subcontract with a particular source or direct a contractor to exclude a source from consideration for a subcontract**
  - **Qualified suppliers: head of an agency may establish SCRM qualification requirements and restrict the procurement to sources that meet such qualification requirements.**
- **Section 806 permits limiting the disclosure of information relating to the basis for excluding a source if risk to national security due to disclosure is greater than risk due to nondisclosure.**

Approved for Public Release
15-MDA-8354 (12 August 15)

From *The World Is Flat* by Thomas Friedman

Dell Inspiron 600m Notebook: Key Components and Suppliers

Component		Supplier or Potential Suppliers
Intel Microprocessor		US-owned factory in the Philippines, Costa Rica, Malaysia, or China *(Intel)*
Memory		South Korea *(Samsung)*, Taiwan *(Nanya)*, Germany *(Infineon)*, or Japan *(Elpida)*
Graphics Card		China *(Foxconn)*, or Taiwanese-owned factory in China *(MSI)*
Cooling fan		Taiwan *(CCI and Auras)*
Motherboard		Taiwan *(Compal and Wistron)*, Taiwanese-owned factory in China *(Quanta)*, or South Korean-owned factory in China *(Samsung)*
Keyboard		Japanese company in China *(Alps)*, or Taiwanese-owned factory in China *(Sunrex and Darfon)*
LCD		South Korea *(Samsung, LG.Philips LCD)*, Japan *(Toshiba or Sharp)*, or Taiwan *(Chi Mei Optoelectronics, Hannstar Display, or AU Optronics)*
Wireless Card		Taiwan *(Askey or Gemtek)*, American-owned factory in China *(Agere)* or Malaysia *(Arrow)*, or Taiwanese-owned factory in China *(USI)*
Modem		China *(Foxconn)*, or Taiwanese company in China *(Asustek or Liteon)*
Battery		American-owned factory in Malaysia *(Motorola)*, Japanese company in Mexico, Malaysia, or China *(Sanyo)*, or South Korean or Taiwanese factory *(SDI and Simplo)*
Hard Disk Drive		American-owned factory in Singapore *(Seagate)*, Japanese-owned company in Thailand *(Hitachi or Fujitsu)*, or Japanese-owned company in the Philippines *(Toshiba)*
CD/DVD		South Korean company with factories in Indonesia and Philippines *(Samsung)*, Japanese-owned factory in China or Malaysia *(NEC)*, Japanese-owned factory in Indonesia, China, or Malaysia *(Teac)*, or Japanese-owned factory in China *(Sony)*
Notebook Carrying Bag		Irish company in China *(Tenba)*, or American company in China *(Targus, Samsonite, and Pacific Design)*
Power Adapter		Thailand *(Delta)*, or Taiwanese-, South Korean-, or American-owned factory in China *(Liteon, Samsung, and Mobility)*
Power Cord		British company with factories in China, Malaysia, and India *(Volex)*
Removable Memory Stick		Israel *(M-System)*, or American company with factory in Malaysia *(Smart Modular)*

What are We Protecting?

Program Protection Planning

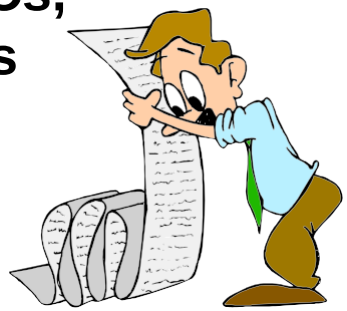
DODI 5000.02 Update

Technology DoDI 5200.39	Components DoDI 5200.44	Information* DoDI 5200.39 DoDI 5200.44
What: Leading-edge research and technology Who Identifies: Technologists, System Engineers ID Process: CPI Identification Threat Assessment: TTRA, MDCITA Counter Measures: AT, Classification, Export Controls, Security, etc. Focus: "Keep secret stuff in" by protecting any form of technology	What: Mission-critical functions and components Who Identifies: System Engineers, Logisticians ID Process: Criticality Analysis Threat Assessment: DIA SCRM TAC Counter Measures: SCRM, SSE, Anti-counterfeits, software assurance, Trusted Suppliers, etc. Focus: "Keep malicious stuff out" by protecting key mission components	What: Information about applications, processes, capabilities and end-items Who Identifies: All ID Process: Various Threat Assessment: Various Counter Measures: Information Assurance, Classification, Export Controls, Security, etc. Focus: "Keep critical information from getting out" by protecting data

Protecting Warfighting Capability Throughout the Lifecycle

What is Critical?

- **To execute policy and guidance beyond identifying ASICs, programs need to identify critical functions/components**
  - Programs lack visibility into most of the MicroE used in systems
  - Prior to Critical Design Review (CDR), configuration and sources of supply are uncertain
  - Technology Development Strategy (TDS) will have many gaps



- **Per MIL-HDBK-61A(SE), Configuration Management Guidance: "Designating *(MicroE Critical Components (CCs))* as Configuration Items increases their visibility and management control throughout the development and support phases."**
- **To enable DoDI 5200.44 and DAG Chapter 13 compliance for Level I and II CCs, need system configuration data prior to CDR and Bill of Material (BOM) information after CDR**

Proposition: During program development, advise contractors and their suppliers of program risk criteria for *MicroE* and require them to identify and nominate CCs based on criticality analysis

Criticality Analysis Methodology

Inputs:
- Initial Capabilities Document
- Capability Development Document
- Capability Production Document
- Concept of Operations
- Concept of Employment
- Data Flow Diagrams
- Software development processes
- Sources and performance experience of key data handling components
- System architecture diagrams down to component level
- Verification plans

Leverage existing mission assurance analysis, including flight & safety critical

Include components with unmediated comms w/critical functions or initial start conditions

Identify and Group Mission Threads by Priority

↓

Identify Critical Functions Assign Criticality Levels

↓

Map Threads and Functions to Subsystems and Components

↓

Assign Criticality Levels

Level I: Total Mission Failure

Level II: Significant/Unacceptable Degradation

Level III: Partial/Acceptable Degradation

Level IV: Negligible

Identify Special Operating Environments and ICT

↓

Identify Critical Suppliers

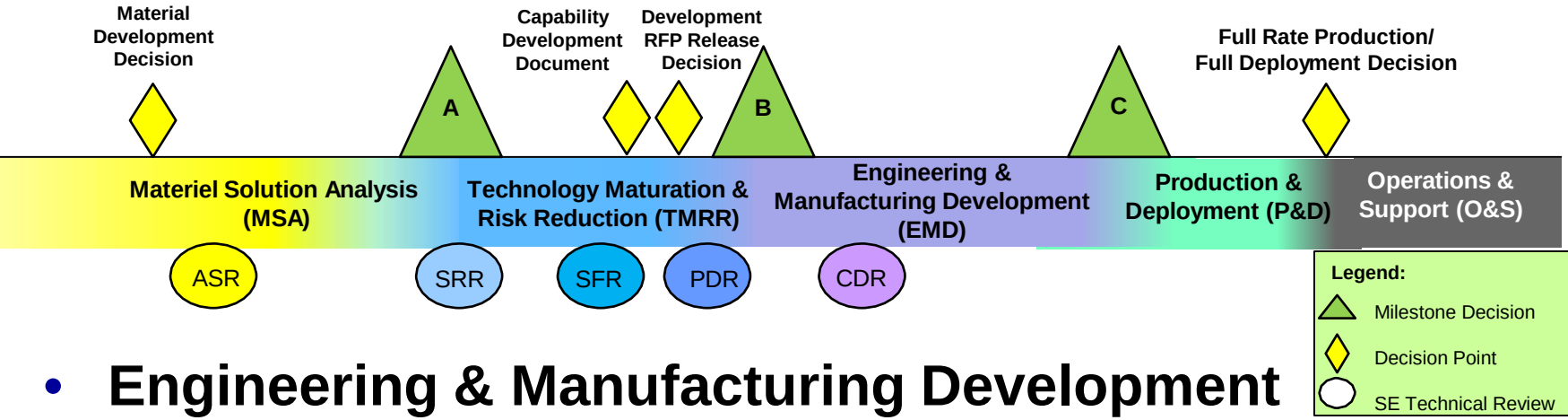
↓

Outputs:
- Table of Level I & II Critical Functions and Components
- Supplier identification

Approved for Public Release
15-MDA-8354 (12 August 15)

Program Protection Plan Milestones

- **Technology Development**
  - Document probable CCs and potential countermeasures
  - Plan life-cycle sustainment of proposed technologies



- **Engineering & Manufacturing Development**
  - Protect CCs by implementing appropriate techniques
- **Production & Deployment**
  - Control product baseline for Class 1 configuration changes
- **Operations & Support**
  - Manage CCs life-cycle and configuration

Configuration → CDR → Parts

Approved for Public Release
15-MDA-8354 (12 August 15)

Sample SCRM SOW Language

IAW DoDI 5200.44 the contractor shall assist the government in conducting Criticality Analyses to identify mission critical functions and Information and Communications Technology (ICT) critical components of the BMDS system elements as requested.
The contractor shall submit to and participate in unannounced government audits into their supply chain activities.
The contractor shall only procure logic bearing components from the vendors approved by the Defense Microelectronic Activity (DMEA) list or request an exception in writing to the government COTR and MDA DE/I with a justification as to why the component could not be procured from the DMEA list.

The contractor shall demonstrate that the contractor has visibility into its supply chain for critical components, understands the risks to that supply chain, and has implemented or plans to implement risk mitigations to counter those risks documented in the PPIP. The Contractor shall flow down requirements for supply chain risk management to subcontractors and lower tier vendors and report discrepancies to the MDA Supply Chain Risk Management/Trusted Systems and Networks Integration Council (MSTIC).

The contractor shall continuously monitor the Program Critical Components List for impact of MDA SCRM Advisories, GIDEP Alerts, or any other similar information from other programs. Critical components affected by these alerts shall not be used without additional analysis and approval by the MDA Supply Chain Risk Management/Trusted Systems and Networks Integration Council (MSTIC). Any critical component or supply chain vulnerability issue discovered by the contractor in the course of development shall be reported to the MSTIC for review. The contractor should develop and submit the appropriate report to the Missile Defense Agency documenting any identified vulnerabilities to the supply chain or individual critical components.

All contractors shall prepare a Supply Chain Risk Management Impact Statement for each MDA SCRM Advisory for which a response is required containing the following:
a. MDA SCRM Advisory Number,
b. Points of Contact for Information,
c. Element or Program affected,
d. Impact on program,
e. Action taken.

Impact statements shall be submitted to the MDA SCRM Advisory Coordinator listed on the advisory. The contractor shall follow any other instructions for response as listed on the advisory.

Many Supply Chain Risks to Consider

Fraudulent Product	Malicious Insertion	Anti-Tamper	Quality Escape	Reliability Failure	Emerging Threats
Counterfeit and other than genuine and new devices from the legally authorized source including relabeled, recycled, cloned, defective, out-of-spec, etc.	The intentional insertion of malicious hard/soft coding, or defect to enable physical attacks or cause mission failure; includes logic bombs, Trojan 'kill switches' and backdoors for unauthorized control and access to logic and data	Unauthorized extraction of sensitive intellectual property using reverse engineering, side channel scanning, runtime security analysis, embedded system security weakness, etc.	Product defect/ inadequacy introduced either through mistake or negligence during design, production, and post-production handling resulting in the introduction of deficiencies, vulnerabilities, and degraded life-cycle performance	Mission failure in the field due to environmental factors unique to military and aerospace environment factors such as particle strikes, device aging, hot-spots, electro-magnetic pulse, etc.	New threats, counterfeit trends, security attacks, and trust issues that combine two or more threats

Proposition: Risk Assessment approach must be integrated to address all

SCRM Advisory:
Hardware Trojan Technology Analysis/Capability

- **Four papers from The People's Liberation Army Information Engineering University (China) were translated and published by the Open Source Center.**
- **The study notes that attackers can utilize a secret path to trigger the intended security flaw inside the FPGA. These events are sensor-based and are conditional.**
- **Attackers have two options to execute the intended security flaw through external and internal triggers.**
- **Compared to SW vulnerabilities, HW vulnerabilities not only have a stronger attack capability, but also are harder to detect and eliminate.**
- **While SW bugs can be fixed through updates, HW Trojans are fixed and work at the lowest level of a computer system and cannot always be detected through SW detection methods.**

SCRM Advisory (Cont):
Next Steps

- **Gather specific engineering and vulnerability data from NSA and the scientific community**
- **Discuss mitigation strategies at the MDA SCRM Trusted System Integration Council (MSTIC) for review, consideration and implementation**
- **Formulate mitigation strategies based on how the FPGAs are being used, exploitation risk, and functionality and association with Critical Program Information (CPI) or critical components for each program**
- **Decide on courses of action that are applicable and tailored for each program**

PPP Lifecycle

Review:
- Concept
- Design
- Materials
- Manufacturing
- Integration
- Operational environment

Providing:
- State of the art
- New or enhanced military capability

CPI/CF/CC Identification and Analysis

Analyze and Identify:
- Mission threads
- Supporting functions
- CC/CF by format and location
- CPI by format and location
- Baseline/interim countermeasures at all locations

MDCITA/TTRA/DIA TAC
- CPI/CC by format and location
- Which systems CPI/CC resides on
- Critical functions related to CPI/CC

Program Submits Threat Requests

Vulnerability Assessment (Independent of IC Threat)
- Spec analysis
- Requirement gap analysis
- OPSEC plan
- Acquisition plan
- C&A
- DSS report
- Existing threat reporting
- History
- TRL
- CERT

MDCITA/TTRA/TAC
- Intent
- Capability

Threat Provided

Threat Probability

Vulnerability (Incorporate IC Threat if available)
- Nature/format
- Paths to CPI at all locations

Monitor residual risk

Risk Assessment

Residual Risk

Potential for undesirable event
Protection priorities
- Risk to mission (component)
- Risk to system
- Risk to enterprise (battlefield scenarios)

Tailored to CPI

Countermeasure

Cost

Integrate security disciplines

PPP

Acronyms:
- C&A certification and accreditation
- CC-critical components
- CERT-Computer Emergency Response Team
- CF-critical functions
- CISP-counterintelligence support plan
- CPI-critical program information
- DSS-Defense Security Service
- IC-intelligence community
- MDCITA-multi-disciplinary counterintelligence threat assessment
- PPIP-program protection implementation plan
- PPP-program protection plan
- TRL-technology readiness level
- TTRA-targeted technology risk assessment

Approved for Public Release
15-MDA-8354 (12 August 15)

System/Software Assurance vs. Info Assurance (Cyber Security)

- System assurance is the justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle.
- Software assurance is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner. *Source: Committee on National Security Standards. CNSS Instruction No. 4009, National Information Assurance Glossary, Ft. Meade, MD, Revised 2010..*
- Information Assurance consists of measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. *Source: Committee on National Security Standards. CNSS Instruction No. 4009, National Information Assurance Glossary, Ft. Meade, MD, Revised 2010..*

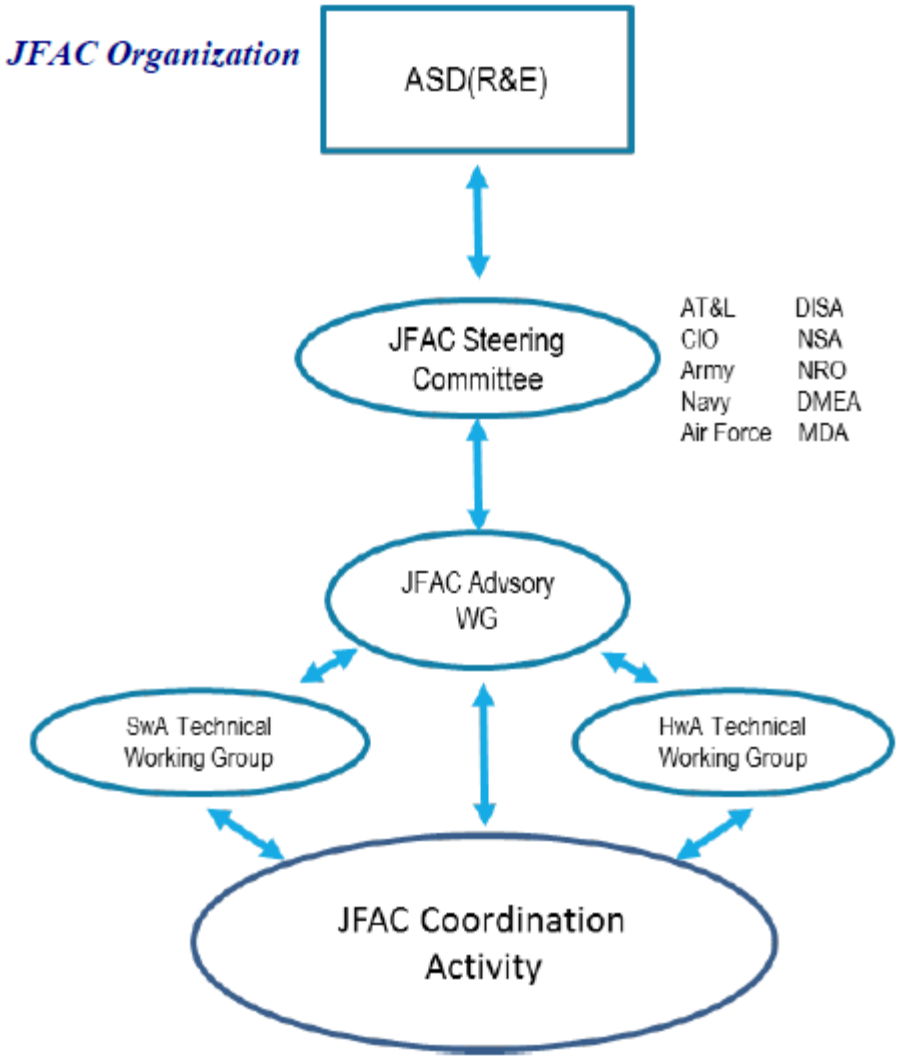
Critical Logic Bearing Component Scrap vs. Demilitarization

- **A 2014 compliance audit revealed a potential vulnerability in the way contractors are disposing of critical components that may contain critical program information.**
- **All microelectronic components need to be demilitarized (destroyed) rather than scrapped.**
  - **Scrapping presents opportunities for reuse and counterfeiting. Also potential for loss of digital information contained on chips.**
  - **The best method for demilitarization of microelectronics is pulverization.**
  - **There is no approved method to degauss, over-write or sanitize for sensitive or critical digital information**
- **Class B changes to parts.**

Joint Federated Assurance Center

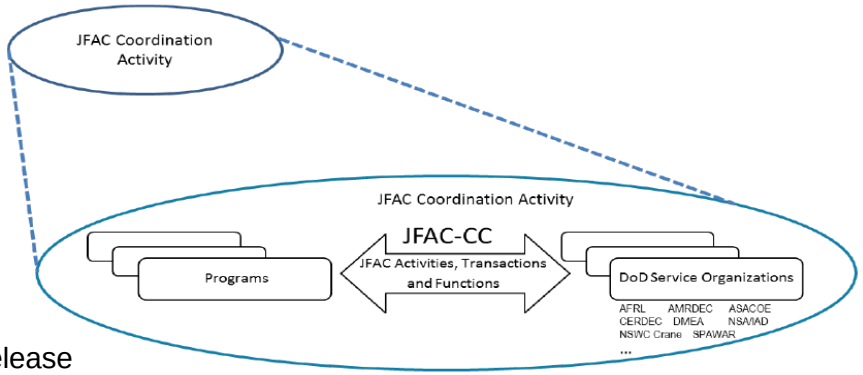
- **Congressionally mandated in 2014, Initial Operational Capability in 2015**
- **MDA is represented on Executive Steering Committee, the Advisory Council, and on both the Software and Hardware Working Groups.**
  - **Chartered to provide testing and reverse engineering services on microelectronics for all of DoD**
  - **Fee for Service**
  - **Shares lessons learned and CM development**
- **Potential Pilots**

JFAC Organization



JFAC Members and Stakeholders

- Office of the Undersecretary of Defense for Acquisition, Technology and Logistics [OUSD(AT&L)]
- DoD Chief Information Officer (CIO)
- Department of the Army
- Department of the Navy
- Department of the Air Force
- National Security Agency (NSA)
- National Reconnaissance Office (NRO)
- Defense Information Systems Agency (DISA)
- Missile Defense Agency (MDA)
- Defense Microelectronics Activity (DMEA)



Backup

Policy and Guidance

- **POTUS National Strategy for Global Supply Chain Security, dated Jan 2012**
- **Presidential Comprehensive National Cyber-Security Initiative (CNCI) 11, dated May 2009 * Derived from NSPD-54/HSPD 23**
- **National Defense Authorization Act (NDAA) for FY 09 Section 254-Trusted Defense Systems**
- **NDAA for FY 11 Section 806-Requirements For Information Relating To Supply Chain Risk**
- **NDAA for FY 11 Section 932-Strategy On Computer Software Assurance**

Public Law

Policy and Guidance (Con't)

- **USD (AT&L) Memo, Subject Document Streamlining - Program Protection Plan (PPP), dated 18 Jul 11**
- **DASD-SE Program Protection White Paper, dated Oct 11**
- **Key Practices Guide for SCRM, OASD(NII)-CIO/ODASD(CIIA), dated Feb 10 * Implementation Document**
- **FY 12 Defense Policy and Planning Guidance**
- **Defense Acquisition Guidebook, Chapter 13, dated Jan 12**

OSD Guidance

- **DoDI 5200.44, Trusted Systems and Networks (TSN), dated 5 Nov 12 * Incorporates and Cancels DTM 09-016**
- **DoDI 5200.39, Critical Program Information (CPI) Protection Within the Department of Defense w/ Change 1, dated 28 Dec 2010**
- **DoDI 5240.24, Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA), dated 8 Jun 2011**

Requirements

JFAC Roles

- Support program offices throughout the life cycle with SwA and HwA expertise, capabilities, policies, guidance, and best practices
- Coordinate with DoD organizations and activities that are developing, maintaining, and offering software and hardware vulnerability detection, analysis, and remediation support
- Conduct SwA and HwA analyses and assessments in support of defense acquisition, operations and sustainment activities
- Advocate for the advancement of DoD interests in SwA and HwA research, development, and test and evaluation activities
- Build relationships with other communities of interest and practice in SwA and HwA such as other government organizations, academic environments, and private industry
- Identify, operationalize, and institutionalize the Department's SwA and HwA capabilities in support of program management offices and other stakeholders.
- Evaluate the need for and impact of DoD investments in support of various SwA and HwA needs and interests.
- Collaborate across the DoD to influence R&D investments and bridge gaps in SwA and HwA capabilities