System Security Engineering and Comprehensive Program Protection

Melinda Reed

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

16th Annual NDIA Systems Engineering Conference

Arlington, VA | October 30, 2013

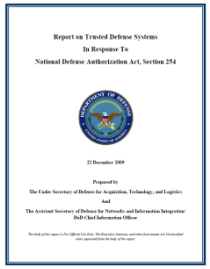
Trusted Defense Systems and Networks Strategy

Drivers/Enablers

- National Cybersecurity Strategies
- Globalization Challenges
- Increasing System Complexity
- Intellectual Property Protection

Delivering Trusted Systems

Report on Trusted Defense Systems



USD(AT&L)
ASD(NII)/DoD CIO

Executive Summary:
http://www.acq.osd.mil/se/pg/spec-studies.html

Ensuring Confidence in Defense Systems

- ***Threat*: Nation-state, terrorist, criminal, or rogue developer who:**
  - Gain control of systems through supply chain opportunities
  - Exploit vulnerabilities remotely
- ***Vulnerabilities***
  - All systems, networks, and applications
  - Intentionally implanted logic
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- ***Traditional Consequences*: Loss of critical data and technology**
- ***Emerging Consequences*: Exploitation of manufacturing and supply chain**
- **Either can result in corruption; loss of confidence in critical**

Today's acquisition environment drives the increased emphasis:

Then		Now
Stand-alone systems	>>>	Networked systems
Some software functions	>>>	Software-intensive
Known supply base	>>>	Prime Integrator, hundreds of suppliers
CPI (technologies)	>>>	CPI and critical components

What Are We Protecting?

Program Protection Planning

DODI 5000.02 Update

DoDI 5200.39 Change 1, dated Dec 2010	DoDI 5200.44	DoDI 8500 Series DoDI 8582.01
Technology	**Components**	**Information**
What: Leading-edge research and technology Who Identifies: Technologists, System Engineers ID Process: CPI Identification Threat Assessment: Foreign collection threat informed by Intelligence and Counterintelligence assessments Countermeasures: AT, Classification, Export Controls, Security, Foreign Disclosure, and CI activities Focus: "Keep secret stuff in" by protecting any form of technology	What: Mission-critical elements and components Who Identifies: System Engineers, Logisticians ID Process: Criticality Analysis Threat Assessment: DIA SCRM TAC Countermeasures: SCRM, SSE, Anti-counterfeits, software assurance, Trusted Foundry, 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: CPI identification, criticality analysis, and classification guidance Threat Assessment: Foreign collection threat informed by Intelligence and Counterintelligence assessments Countermeasures: Information Assurance, Classification, Export Controls, Security, etc. Focus: "Keep critical information from getting out" by protecting data

Protecting Warfighting Capability Throughout the Lifecycle

SSE Priorities

- **Policy Initiatives**
  - DoDI 5000.02 Operation of the Defense Acquisition System
  - DoDI 5200.39 Critical Program Information (CPI) Protection Within the DoD
  - DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks
  - DoDI 8500.01E Information Assurance
- **Depth of PPP Analysis throughout the Life Cycle**
- **Protection of Integrated Circuits**
- **Software Assurance**
- **Protection of Defense Industrial Base Systems**
- **Incorporating SSE into Contracts**
- **Program Protection Guidance**
- **Integrated SSE**

DoD efforts are targeting integration of system security engineering considerations throughout the system life cycle

Program Protection Integrated in Policy

DoDI 5000.02 Operation of the Defense Acquisition System

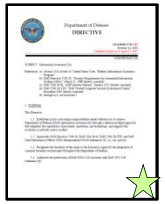
- Regulatory Requirement for Program Protection Plan at Milestones A, B, C and FRP/FDD
- References DoDI 5200.39

DoDI 5200.39 Critical Program Information (CPI) Protection Within the DoD

- Assigns responsibility for Counterintelligence, Security, and System Engineering support for the ID and protection of CPI
- Expands definition of CPI to include degradation of mission effectiveness

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 <u>vulnerabilities in system design</u> or <u>subversion of mission critical functions or components</u>



DoDI 8500.01E Information Assurance

- Establishes policy and assigns responsibilities to achieve DoD information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare

☆ - Update underway

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

DoDI 5200.44
Trusted Systems and Networks

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").

- **Implements the DoD's Trusted Systems and Networks (TSN) strategy**
- **Manage risk of mission-critical function and component compromise throughout lifecycle of key systems by utilizing**
  - Criticality Analysis as the systems engineering process for risk identification
  - Countermeasures: Supply chain risk management, software assurance, secure design patterns
  - Intelligence analysis to inform program management
- **Codify trusted supplier requirement for DoD-unique application-specific integrated circuits (ASICs)**
- **Document planning and accomplishments in program protection and information assurance activities**

PPP Analysis Level of Detail through the Life Cycle (SETR)

	ASR	SRR	SFR	PDR	CDR	SVR/FCA
System Specification Level	• ICD / Comments on Draft CDD (if avail) • Prelim System Performance Spec • Sys model/arch including CONOPS, i/f, & operational/ functional requirements	• System Performance Spec • Verifiable sys req'ts detailed to enable functional decomposition • Req. traceability • External i/f documented	• Functional Baseline • System functions decomposed and mapped to System elements • Sys elements defined • Preliminary allocation of functions optimized	• Allocated Baseline • Preliminary design (fct and i/f) for all elements (HW & SW) complete • HW – Verifiable component characteristics • SW – CSCs, CSUs	• Initial Product Baseline • Detailed design & i/f for comp/unit production and test • HW– Physical (form fit, function) • SW– CSU level design	• SVR– System performance verified to meet functional & allocated baselines • Product Baseline for initial production
Criticality Analysis (CA)	Mission based functions	System requirements level functions	Subsystem level subfunctions	Assembly/ component	Component/ part	Part (prelim)
Vulnerability Assessment (VA)	Response to tutorial questions	System function level response to tutorial questions	Subsystem level responses	Assembly / Component level responses	component level responses	Part level responses (prelim)
Risk Assessment (RA)	• Objective risk criteria established • Applied at function level	• Risk criteria updated • applied at system level	Risk criteria updated & applied at subsystem level	Risk criteria updated & applied at assembly level	Risk criteria updated & applied at component level	Risk criteria updated & applied at prelim part level of critical components
Counter-measure (CM)	Risk based supply chain, design and SW CM in RFP	Risk based system function level CM selection	Risk based subsystem function level CM selection	Risk based assembly level CM selection	Risk based component level CM selection	Risk based part level CM selection
IA / Cyber security	• System Categorization/Registration • Initial Controls & tailoring	Risk based control strength of implementation determined	• IA Control trace to spec • Additional IA Controls tailoring/trades as CM if needed	• IA Control trace to spec • Additional IA Controls as CM if needed • IA/IA enabled Components ID'd as CM	• IA controls incorporated traced to physical baseline • Controls Assessed and discrepancies ID'd/categorized	• IA controls incorporated traced to product baseline • IAVM program established for IA control maintenance
RFP	• CM and IA controls incorporated into TD SOW and SRD		CM and IA controls incorporated into EMD SOW and SRD		CM and IA controls incorporated into Production SOW and SRD	

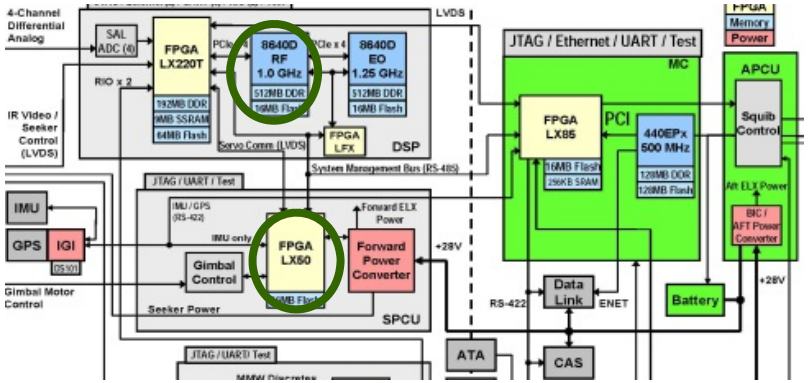
PPP Analysis Level of Detail through the Life Cycle (Milestones)

	Milestone A	Pre-EMD	Milestone B	Milestone C	FRP/PCA/FDD
PPP Analysis	Same level as ASR analysis	Same level as SRR and SFR	Same level as PDR	Same level as CDR and SVR	• PCA Est. Product Baseline • Critical function component bill of material (BOM)
Criticality Analysis (CA)	"	"	"	"	Part
Vulnerability Assessment (VA)	"	"	"	"	Part level responses
Risk Assessment (RA)	"	"	"	"	Risk criteria updated & applied at BOM level critical components
Countermeasure (CM)	"	"	"	"	Risk based part level CM selection
IA / Cyber security	"	"	"	"	• IA controls incorporated traced to product baseline and BOM • IAVM program established for IA control maintenance
RFP	CM and IA controls incorporated into TD SOW and SRD	CM and IA controls incorporated into EMD SOW and SRD		CM and IA controls incorporated into Production SOW and SRD	

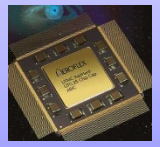
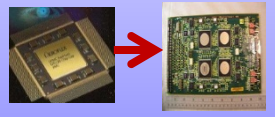
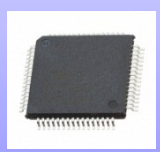
Misuse Mission Scenario Evaluation during Requirements Analysis

Misuse Mission Scenarios are used to analyze the mission consequences of exploitation of a system, supply chain or development environment vulnerabilities to determine protection requirements

Possible Failure Description			Exploit				Risk Assessment	
Event	Triggering Event	Consequence	Perspec-tive	Autono-mous	Triggered		In-Place CM	Residual Risk
Weapon cannot guide to target	Mission Controller malicious insertion	- Missed target - Collateral damage	Insider				Controller OEM Diversity	Low



Notional Use Cases and Countermeasures for Integrated Circuits

	Use Case 1:	Use Case 2:	Use Case 3:
Use Cases	**Custom ASIC** that has a specific DoD military end use 	**ASIC in a COTS assembly** that is primarily intended for commercial market 	**MOTS/GOTS Integrated Circuit (IC)** that has a DoD end use 
Countermeasures	• Use Trusted Supply Flow (Trusted Supplier) for design, mask, fabrication, packaging and testing	• Perform supply chain risk assessment of ASICs if the COTS assembly is determined as a critical component • Implement SCRM countermeasures commensurate with assessed risk	• Consider source and employment history • Apply countermeasures commensurate with assessed risk, including enhanced/focused testing • Use trusted supplier and product flow as applicable, such as FPGA programming services; • Use DMEA accredited trusted supplier and trusted product flow if ASIC

Software Assurance (SwA)

- **SwA is a fundamental element of DoD's Trusted Systems and Networks policy and procedures and DoD acquisition**
- **DoD cyber policies enhance the focus on Software Assurance**
  - Policy documents are being updated to address evolving SW Assurance tools, methodologies, and to address statutes
  - Guidance for SW Assurance is being updated to support programs across the life cycle
- **The SwA CoP is important to the DoD's growing competence in SwA**
  - Participate in development and promulgation of enabling guidance, tools, methods
  - Assist in coordination and building partnerships across the DoD, and with external organizations
  - Become a SME resource for Program Management teams to support SwA planning and vulnerability risk mitigation

FY 12 Accomplishments

- Established DoD SwA enterprise-level Community of Practice (CoP) with DCIO(CS)/TMSN and NSA(CAS)
- Initiated three DoD SwA stakeholder initiatives:
  - SwA-related contract language
  - DoD Enterprise coordination and information sharing
  - Workforce education and training
- Updated SwA elements of the Defense Acquisition Guidebook to assist acquisition programs in tailoring and refining software security requirements
- Initiated a study of SwA tools for development and operational testing
- Agreed upon a standard definition of SwA across the Department

FY 13 Goals

- Expand the DoD SwA Community of Practice to increase coordination, collaboration, and promulgation of best practices
- Update policy, guidance, and PPP activities to address software assurance in software development and system operation
- Assess state-of-the-art in commercially available SW vulnerability detection and analysis tools and methodologies

Defense Industrial Base (DIB) Cyber Security

"The private sector, government, military, our allies - all share the same global infrastructure and we all share the responsibility to protect it."

- Secretary of Defense Leon E. Panetta

Thursday, October 11, 2012

DoD efforts to advance cyber security in the DIB include:

- DIB Cyber Security/Information Assurance (CS/IA) Program, and its optional enhanced component the DIB Enhanced Cybersecurity Services (http://dibnet.dod.mil)
- Standards development in collaboration with Industry
- Reinforcing protection of technical information in acquisition activities

RFP Sections

RFP Package

- Section A: Solicitation Contract Form
- Section B: Supplies or services and prices/costs
- **Section C: Description/specifications/work statement**
  - **System Requirements Document (SRD - SPEC)**
  - **Statement of Work (SOW)**
  - **Contract Deliverable Requirements List (CDRLs)**
- Section D: Packaging and marking
- Section E: Inspection and Acceptance
- Section F: Deliveries or performance
- Section G: Contract administration data
- Section H: Special contract requirements
- Section I: Contract Clauses
- Section J: List of Documents, Exhibits, and other Attachments
- Section K: Representations, Certification, and Other Statements of Offerors
- **Section L: Instructions, conditions, and notices to offerors**
- **Section M: Evaluation factors for award**

- **Incorporate Design Protections**
  System Requirements Document (SRD), Specification, or equivalent
- **Incorporate Process Protections**
  Statement of Work (SOW), Statement of Objectives (SOO), Performance Work Statement (PWS), or equivalent
- **Contract Deliverable Requirements List (CDRLs)**
  Data Item Description (DID)

- **Description of program protection processes for Level I and Level II critical components**
  Sections L and M

Program Protection Guidance

Program Protection Plan Outline & Guidance, dated 18 Jul 2011

- **Focal point for documenting Program security activities, including:**
  - Plans for identifying and managing risk to CPI and critical functions and components
  - Responsibilities for execution of comprehensive program protection
  - Tables of actionable data, not paragraphs of boilerplate
  - End-to-end system analysis and risk management
- **http://www.acq.osd.mil/se/docs/PPP-Outline-and-Guidance-v1-July2011.pdf**

Defense Acquisition Guidebook Chapter 13, "Program Protection"

- **Provides implementation guidance for TSN Analysis and CPI Protection**
- **Describes SSE activities throughout the Defense Acquisition Life Cycle**
- **https://acc.dau.mil/dag13**

In Summary

- **Holistic approach to security is critical**
  - To focus attention on the threat
  - To avoid risk exposure from gaps and seams
- **Program protection policy provides overarching framework for trusted systems**
  - Common implementation processes are beneficial
- **Stakeholder integration is key to success**
  - Acquisition, CIO, Intelligence, Engineering, Industry, Academic communities are all stakeholders
- **Systems engineering brings these stakeholders, risk trades, policy, and design decisions together**
  - Informing leadership early; providing programs with risk-based options

For Additional Information

Melinda Reed

ODASD, Systems Engineering

571-372-6562 | Melinda.K.Reed4.civ@mail.mil

Systems Engineering: Critical to Defense Acquisition










Innovation, Speed, Agility

http://www.acq.osd.mil/se