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

Prioritize by Mission Dependence

Comprehensive Program Protection Planning

Enhance R&D for Vulnerability Detection and Response

Partner with Industry

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 warfighting capability

---

**Today’s acquisition environment drives the increased emphasis:**

<table>
<thead>
<tr>
<th>Then</th>
<th>Now</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stand-alone systems</td>
<td>Networked systems</td>
</tr>
<tr>
<td>Some software functions</td>
<td>Software-intensive</td>
</tr>
<tr>
<td>Known supply base</td>
<td>Prime Integrator, hundreds of suppliers</td>
</tr>
<tr>
<td>CPI (technologies)</td>
<td>CPI and critical components</td>
</tr>
</tbody>
</table>
**What Are We Protecting?**

### Technology
- **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

### Components
- **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

### Information
- **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**

---

**Program Protection Planning**

*DoDI 5000.02 Update*

---

**DoDI 5200.39**
Change 1, dated Dec 2010

**DoDI 5200.44**

**DoDI 8500 Series**
DoDI 8582.01
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 vulnerabilities in system design or subversion of mission critical functions or components

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

• 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)**

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

**Distribution Statement A – Approved for public release by OSR on 10/28/2013, SR Case # 14-S-0136 applies. Distribution is unlimited.**
## PPP Analysis Level of Detail through the Life Cycle (Milestones)

<table>
<thead>
<tr>
<th>Milestone</th>
<th>Milestone A</th>
<th>Pre-EMD</th>
<th>Milestone B</th>
<th>Milestone C</th>
<th>FRP/PCA/FDD</th>
</tr>
</thead>
</table>
| 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 Scenarios** are used to analyze the mission consequences of exploitation of a system, supply chain or development environment vulnerabilities to determine protection requirements.

<table>
<thead>
<tr>
<th>Possible Failure Description</th>
<th>Exploit</th>
<th>Risk Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event</td>
<td>Triggering Event</td>
<td>Consequence</td>
</tr>
</tbody>
</table>
| 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

<table>
<thead>
<tr>
<th>Use Cases</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use Case 1:</strong> Custom ASIC that has a specific DoD military end use</td>
<td>• Use Trusted Supply Flow (Trusted Supplier) for design, mask, fabrication, packaging and testing</td>
</tr>
</tbody>
</table>
| **Use Case 2:** ASIC in a COTS assembly that is primarily intended for commercial market | • Perform supply chain risk assessment of ASICs if the COTS assembly is determined as a critical component  
  • Implement SCRM countermeasures commensurate with assessed risk |
| **Use Case 3:** MOTS/GOTS Integrated Circuit (IC) that has a DoD end use | • 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

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](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