System Security Engineering and Program Protection Integration into SE

Melinda Reed
Deputy Director for Program Protection
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

17th Annual NDIA Systems Engineering Conference
Springfield, VA | October 29, 2014
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, and/or degrade system behavior

• **Vulnerabilities:**
  – All systems, networks, and applications
  – Intentionally implanted logic
  – Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)

• **Consequences:**
  – Loss of critical data and technology
  – System corruption
  – Loss of confidence in critical warfighting capability; mission impact

*Access points are throughout the lifecycle…*

*…and across multiple supply chain entry points*

- Government
- Prime, subcontractors
- Vendors, commercial parts manufacturers
- 3rd party test/certification activities
Many Program Protection Risks to Consider

Quality Escape
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.

Reliability Failure
Mission failure in the field due to environmental factors unique to military and aerospace environment factors such as particle strikes, device aging, hot-spots, electromagnetic pulse, etc.

Fraudulent Product
Counterfeit and other than genuine and new devices from the legally authorized source including relabeled, recycled, cloned, defective, out-of-spec, etc.

Malicious Insertion
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.

Anti-Tamper
Unauthorized extraction of sensitive intellectual property using reverse engineering, side channel scanning, runtime security analysis, embedded system security weakness, etc.

Emerging Threats
New threats, cyber security attacks, and trust issues that combine two or more threats.

DoD Program Protection focuses on risks posed by adversary actors.
Program Protection in Context

• **Program Protection:** The integrating process for managing risks to advanced technology and mission-critical system functionality from foreign collection, design vulnerability or supply chain exploit/insertion, and battlefield loss throughout the acquisition lifecycle.

  *PPP Outline and Guidance*

• **Systems Security Engineering:** An element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities.

  *DoDI 5200.44*

• **Critical Program Information (CPI):** Elements or components of a research, development, and acquisition (RDA) program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability.

  *DoDI 5200.39*

For more information:
http://www.acq.osd.mil/se/pg/policy.html#sa
http://www.acq.osd.mil/se/pg/guidance.html#sa
Program Protection
Interim DoDI 5000.02

• Program Protection is the integrating process for managing risks to DoD warfighting capability from foreign intelligence collection; from hardware, software, and cyber vulnerability or supply chain exploitation; and from battlefield loss throughout the system life cycle.
  – Also supports international partnership building and cooperative opportunities objectives by enabling the export of capabilities without compromising underlying U.S. technology advantages

• Program managers will employ system security engineering practices and prepare a PPP to guide their efforts and the actions of others to manage the risks to critical program information and mission-critical functions and components associated with the program
  – The PPP will be submitted for MDA approval at each Milestone review, beginning with Milestone A

• Program managers will describe in their PPP:
  – Critical Program Information, mission-critical functions, and critical components
  – Threats to and vulnerabilities of these items
  – Plans to apply countermeasures to mitigate associated risks
  – Plans for exportability and potential foreign involvement
  – The Cybersecurity Strategy and Anti-Tamper plan are included as appendices
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

---

**Program Protection Planning**
*Interim DoDI 5000.02*

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

- **DoDI 5200.44**

- **DoDI 8500 Series**
  - DoDI 8500.01E
  - DoDI 8582.01
Program Protection Activity - Integral Part of SE Process

Criticality Analysis
- Determine system critical components based on critical mission threads
- Analyze component vulnerability to malicious exploit
- Identify potential component suppliers

CPI Analysis
- Identify capability elements providing a US technological advantage
- Assess the risk associated with each CPI (exposure, consequence of compromise)
- Horizontal analysis

Program Protection Plan
- Engineering risk/cost trade-off analysis to determine system security requirements
- Determine countermeasures to address vulnerabilities: OPSEC, trusted suppliers, system security engineering, cybersecurity, hardware/software assurance, and anti-tamper

Contractor
- RFP includes supply chain and security requirements
- Continually assess security risks during design reviews and system implementation
- Conduct early defense exportability features planning and design

Threat Assessment
- Analyze Capstone Threat Assessments
- Analyze DIA all-source analysis and threat report
- Analyze foreign collection threats in the technology targeting risk assessment (TTRA)

Test & Evaluation
- Detect HW/SW vulnerabilities
- Evaluate AT protections
- Contractor, DT, OT assessment of mitigations

Acquisition strategy mitigations for supplier threat (e.g., blind buy, trusted source)
Foreign involvement expectations and impacts
SE, SSE and DT&E are Mutually Supportive

**MSA**
- System Requirements, security performance and threat parameters
  - SEP, PPP
  - SE, SSE and DT&E are Mutually Supportive
  - SEP, PPP

**TMRR**
- Preliminary System Design, with critical hardware, software components, vulnerabilities
  - SEP, PPP

**EMD**
- Detailed System Design, with identified known vulnerabilities
  - SEP, PPP

**P&D**
- DT&E Assessment
  - DT&E Assessment

- System Acceptance

- Requirements are translated into industry solicitations throughout the lifecycle
- System

**SE**
- Evaluation Methodology, T&E strategy, schedule, & resources
  - MS-A TEMP

**DT&E**
- DT&E Assessment, Evaluation Framework, T&E strategy, schedule, & resources
  - MS-B TEMP

- Detailed System Design, with identified known vulnerabilities
  - SEP, PPP

- Preliminary System Design, with critical hardware, software components, vulnerabilities
  - SEP, PPP

- System Requirements, security performance and threat parameters
  - SEP, PPP
CPI Protection Throughout the Life Cycle

• **Anti-Tamper (AT)** is the set of system engineering activities (hardware and/or software techniques) designed into the system architecture to protect CPI against:
  – Unwanted technology transfer (e.g. technology loss)
  – Potential adversary countermeasure development
  – System modification to enhance capability/performance

• **Anti-Tamper guidance**
  – An AT Concept prepared at Milestone (MS) A
  – An AT Plan is required at MS B
  – Submitted as an annex to the program’s PPP

Balance CPI exposure — threat — consequence of loss
Protecting Components
DoDI 5200.44

- 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
“America must also face the rapidly growing threat from cyber-attacks… We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy.

“We are going to aggressively protect our intellectual property. Our single greatest asset is the innovation and the ingenuity and creativity of the American people. It is essential to our prosperity and it will only become more so in this century.”

President Barack Obama
February 2013

DoD efforts to advance cyber security in the Defense Industrial Base (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 contract requirements
Safeguarding Unclassified Controlled Technical Information

- **Secretary of Defense Memorandum, October 10, 2013**
  - Emphasizes DoD commitment to preserving the intellectual property (IP) and competitive capabilities of the Defense Industrial Base (DIB) and the technological superiority of our fielded military systems.

- **Key Goals**
  - Protect DoD unclassified controlled technical information from cyber intrusions
  - Minimize the consequences associated with loss of this information

- **Augments current activities**
  - Re-emphasizes the DIB Cyber Security/Information Assurance (CS/IA) Program
DFARS Clause 252.204-7012:
Safeguarding Unclassified Controlled Technical Information*

- **Published November 18, 2013**
  - Clause affects all new contracts that contain, or will contain unclassified controlled technical information
  - Includes flow down to all subcontracts

- **Purpose:** Establish minimum requirements for DoD unclassified controlled technical information on contractor information systems
  - Requires contractors implement minimum set of information security controls
    - 51 information security controls from NIST SP 800-53, Revision 4
    - Combination of Technical, Process, Awareness, and Training measures
  - Requires contractors report cyber incident and compromises
  - Requires contractor actions to support DoD damage assessment as needed

- **Incident Reporting**
  - Reporting includes:
    - DoD contracts and subcontractor information affected by a cyber incident or compromise
    - DoD programs, platforms, or systems involved
    - Description of DoD technical information compromised
  - Reported information does not include signatures or other threat actor indicators

*http://www.acq.osd.mil/dpap/dars/dfars/html/current/204_73.htm*
Major Actions Underway

• **Updating Program Protection guidance and training**
  – Establishing a discipline for system security engineering

• **Implementing DFARS Clause 252.204-7012, “Safeguarding Unclassified Controlled Technical Information”**
  – Working with industry and contracting community
  – Providing guidance, working through procedures

• **Joint Federated Assurance Center for HW/SW**
  – Required by Section 937 of FY14 NDAA
  – Provides network of vulnerability analysis detection and mitigation support to programs; and R&D improvement (resource limited)

• **Trusted microelectronics strategy to move beyond ASICs**
  – FPGAs, Microprocessors, Logic Application Specific Standard Products, Memories, A-D Converters, Interface Chips

• **Anti-Tamper Policy and Guidance updates**
  – DoD Instruction for AT, AT Technology oversight, guidance updates
Our Focus on SSE and SE

• **DoD** is putting policy in place for a risk-based cost benefit trade-off process to protect systems, their supply chain, and their software development

• **DoD** is emphasizing the importance of SSE within systems engineering and its contribution to the design of systems by:
  – Ensuring that program protection is addressed during the SE technical reviews
  – Incorporating program protection and system security engineering requirements and processes into engineering development contracts
  – Working with industry and standards groups revitalize system security engineering

• **Industry** is playing an important role in the DoD SSE initiative by:
  – Investing in research and processes to protect systems, the supply chain and the software development
  – Developing their SE and SSE processes and skills

**DoD efforts are targeting integration of system security engineering considerations throughout the system life cycle**
Systems Engineering: Critical to Defense Acquisition

Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se
For Additional Information

Melinda Reed
ODASD, Systems Engineering
571-372-6562 | Melinda.K.Reed4.civ@mail.mil

Paul Popick
ODASD, Systems Engineering
571-372-6467 | Paul.R.Popick.ctr@mail.mil

JeanPaul LeSaint
ODASD, Systems Engineering
571-372-6554 | JeanPaul.R.LeSaint.ctr@mail.mil
Additional References
### DFARS Clause 252.204-7012: Minimum Security Controls for Safeguarding

<table>
<thead>
<tr>
<th>Access Control (AC)</th>
<th>Configuration Management (CM)</th>
<th>Physical &amp; Environmental (PE)</th>
<th>Program Management (PM)</th>
<th>Risk Assessment (RA)</th>
<th>System and Communication Protection (SC)</th>
<th>System &amp; Information (SI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-6: Least Privilege</td>
<td>CM-8: Information System Component Inventory</td>
<td></td>
<td>SC-28: Protection of Information at Rest</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-7: Unsuccessful Logon Attempts</td>
<td>Contingency Planning Acquisition (CP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-11(1): Session Lock</td>
<td>CP-9: Information System Backup</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-17(2): Remote Access</td>
<td>Identification and Authentication</td>
<td>Identification and Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-20(1): Use of External Information Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-20(2): Use of External Information Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-22: Publicly Accessible Content</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Awareness and Training (AT)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AT-2: Security Awareness Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit and Accountability (AU)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AU-2: Audit Events</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AU-3: Content of Audit Records</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AU-6(1): Audit Review, Analysis and Reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AU-7: Audit Reduction and Report Generation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AU-8: Timestamps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AU-9: Protection of Audit Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• The term includes technical data or computer software of any kind that can be used, or adapted for use, in the design, production, manufacture, assembly, repair, overhaul, processing, engineering, development, operation, maintenance, adapting, testing, or reconstruction of goods or materiel; or any technology that advances the state of the art, or establishes a new art, in an area of significant military applicability in the United States.

  – The data may be in tangible form, such as a blueprint, photograph, plan, instruction, or an operating manual, or may be intangible, such as a technical service or oral, auditory, or visual descriptions.

  – Examples of technical data include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software.
Program Protection Integrated in Policy

**Interim 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) Protection Within the DoD**
- Assigns responsibility for Counterintelligence, Security, and System Engineering support for the identification and protection 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 (including software, microelectronics)

**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 a DoD cybersecurity program to protect and defend DoD information and information technology
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 Protection Requirements and Designs
  System Requirements Document (SRD), Specification, or equivalent

- Incorporate Protection Activities to develop protection requirements, designs and to evaluate those protections
  Statement of Work (SOW), Statement of Objectives (SOO), Performance Work Statement (PWS), or equivalent

- Contract Deliverable Requirements List (CDRLs)
  Contract Data Item with Data Item Description (DID)

- Defense Federal Acquisition Regulation (DFAR)

- As part of the evaluation request a contractor description of their system security protections and the protection activities to be performed during the acquisition.
- Sections L and M
PPP Approval Statistics
Since Outline and Guidance Signed

<table>
<thead>
<tr>
<th>52 PPPs Approved</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY 2010</td>
</tr>
<tr>
<td>FY 2011</td>
</tr>
<tr>
<td>FY 2012</td>
</tr>
<tr>
<td>FY 2013</td>
</tr>
<tr>
<td>FY 2014</td>
</tr>
</tbody>
</table>

FY14 PPPs by Service

Program Protection Outline and Guidance signed 18 July 2011