DoD Trusted Systems and Networks (TSN) Update

Kristen Baldwin
Principal Deputy
Office of the Deputy Assistant Secretary of Defense for Systems Engineering, OUSD(AT&L)

NDIA Systems Engineering Division Meeting
April 17, 2013
Trusted Defense Systems and Networks Strategy

Drivers/Enablers

- National Cybersecurity Strategies
- Congressional Interest
- Globalization Challenges
- Increasing System Complexity
- Increased Threat

Delivering Trusted Systems

Prioritize by Mission Dependence

Comprehensive Program Protection Planning

Enhance R&D, and vulnerability detection and response

Partner with Industry

Report on Trusted Defense Systems

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

Executive Summary:
http://www.acq.osd.mil/se/pg/spec-studies.html
What Are We Protecting?

Program Protection Planning

DoDI 5000.02

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 Life Cycle

DoD 5000.02

DoDI 5200.39

DoDI 5200.44

DoDI 8500 Series

DoDI 8582.01

DoD SE Update
2013/04/17 | Page-3

Distribution Statement A – Approved for public release by OSR, SR Case #s 13-S-1033 and 13-S-1635 apply.
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

DoD Issuances Website: http://www.dtic.mil/whs/directives/corres/ins1.html
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)
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
FY13 NDAA Sections 941 and 933

- **FY13 NDAA SEC. 941: REPORTS TO DEPARTMENT OF DEFENSE ON PENETRATIONS OF NETWORKS AND INFORMATION SYSTEMS OF CERTAIN CONTRACTORS**
  - “The Secretary of Defense shall establish procedures that require each cleared defense contractor to report ... when a network or information system of such contractor that meets the criteria established pursuant to subsection (b) is successfully penetrated.”

- **FY13 NDAA SEC. 933: IMPROVEMENTS IN ASSURANCE OF COMPUTER SOFTWARE PROCURED BY THE DEPARTMENT OF DEFENSE**
  - USD(AT&L), in coordination with the DoD CIO... “shall develop and implement a baseline software assurance policy for the entire lifecycle of covered systems. Such policy shall be included as part of the strategy for trusted defense systems of the Department of Defense.”
  - “(2) require covered systems to identify and prioritize security vulnerabilities and, based on risk, determine appropriate remediation strategies for such security vulnerabilities;”

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
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
Data Vulnerability Tiger Team

- **USD(AT&L) Memorandum, February 7, 2013**
  - Established the Data Vulnerability Tiger Team
  - 60-day schedule
  - Review progress in protecting unclassified technical data
  - Identify further actions to take

**Tiger Team actions**
- Identify Focus Teams
- Focus Teams will analyze gaps and recommend actions
- Consolidate recommendations for USD(AT&L)
Software Assurance

• **FY 12 Activities**
  – Established DoD Software Assurance (SwA) enterprise-level Community of Practice (CoP) in coordination with DCIO(CS)/TMSN and NSA(CAS)
  – Initiated three DoD SwA stakeholder initiatives:
    – SwA-related contract language
    – 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
System Security Community Activities

- **NDIA “Guidebook for System Assurance”, Version 1.0, 2008**
  - Process/technology guidance to increase the level of system assurance through a planned, systematic set of multi-disciplinary activities
- **ISO/IEC 15026 – System and Software Engineering – Systems and Software Assurance**
  - Establishes common assurance concepts, vocabulary, integrity levels and life cycle activities
- **ISO/IEC 27036 – IT Security Techniques – Supplier Relationships**
  - Establishes techniques between acquirer and supplier for supply chain risk management
- **International Council on Systems Engineering (INCOSE) Handbook**
  - Working group to develop security engineering updates to INCOSE SE Handbook
- **NIST - System Security Engineering (SSE) 800-160 Special Pub (In Development)**
  - Aligns SSE with ISO/IEC15288 terminology, incorporates DoD best practices
  - DoD Appendix targets DoD community, includes Systems Engineering Technical Review (SETR) criteria
- **The Open Group (TOG)**
  - The Open Trusted Technology Provider Framework (O-TTPF) - open standard that codifies best practices across the entire lifecycle (targeted against counterfeit HW & malicious SW)
  - [http://www.opengroup.org/ogttf/](http://www.opengroup.org/ogttf/)
• **System Assurance Committee-led Workshop:**
  – Reviewed threat and policy related to trusted defense systems
  – Identified issues for specific areas of PP via 3 focus groups
  – Voted on the Top 5 issues regarding Program Protection

<table>
<thead>
<tr>
<th>Rank</th>
<th>Group</th>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td><strong>Taxonomy</strong></td>
<td>Integration of the DoD security disciplines is hampered by terms of reference that have different meanings depending on the discipline or the context.</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td><strong>Limited Security Performance Metrics are available</strong></td>
<td>Lack of performance metrics to ensure program protection requirements.</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td><strong>Satisfying PPP Objectives through Improved Contract / Acquisition Strategy</strong></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>Lack of well defined threat and attack vectors for SE community in Acquisition and Industry</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>2, 3</td>
<td><strong>Lack of education across the acquisition and industry communities with regards to SSE</strong></td>
<td></td>
</tr>
</tbody>
</table>
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
Systems Engineering: Critical to Acquisition Success

Innovation, Speed, and Agility
http://www.acq.osd.mil/se