Program Protection and Anti-Tamper

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

NDIA Industrial Committee on Program Management (ICPM) Meeting
June 11, 2013
Trusted Defense Systems and Networks Strategy

Drivers/Enablers

- National Cybersecurity Strategies
- Globalization Challenges
- Increasing System Complexity
- Evolving Threat
- U.S. Technical Advantage

Delivering Trusted Systems

Prioritize by Mission Dependence

Comprehensive Program Protection Planning

Enhance R&D for Vulnerability Detection and Response

Partner with Industry

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

Executive Summary:
http://www.acq.osd.mil/se/pg/spec-studies.html
Program Protection (PP) Planning

DoDI 5000.02

DoDI 5200.39

DoDI 5200.44

DoDI 8500 Series
DoDI 8582.01

**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:** Anti-Tamper, Classification, Export Controls, Security, Foreign Disclosure, and CI activities
- **Focus:** “Keep secret stuff in” by protecting any form of technology

**Components**
- **What:** Mission-critical 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 SE Update
2013/06/11 | Page-3

Distribution Statement A – Approved for public release by OSR on 6/7/13, SR Case # 13-S-2164 applies. Distribution is unlimited.
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*

- **System 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
Protecting CPI via Anti-Tamper

• **What is Anti-Tamper (AT)?**
  System engineering activities (hardware and/or software techniques) designed into the system architecture to protect CPI against:
  - Unwanted technology transfer (e.g., technology loss)
  - Countermeasure development
  - Capability/performance enhancement through system modification

• **Why do we need AT?**
  Deter, impede, detect, and respond to the exploitation of CPI in DoD systems resulting from combat losses or export sales.
Achieve Affordable Programs
- Mandate affordability as a requirement
- Institute a system of investment planning to derive affordability caps
- Enforce affordability caps

Control Costs Throughout the Product Lifecycle
- Implement “should cost” based management
- Eliminate redundancy within war-fighter portfolios
- Institute a system to measure the cost performance of programs and institutions and to assess the effectiveness of acquisition policies
- Build stronger partnerships with the requirements community to control costs
- Increase the incorporation of defense exportability features in initial designs

Incentivize Productivity and Innovation in Industry and Government
- Align profitability more tightly with Department goals
- Employ appropriate contract types
- Increase use of Fixed Price Incentive contracts in Low Rate Initial Production
- Better define value in “best value” competitions
- Only use LPTA when able to clearly define Technical Acceptability
- Institute a superior supplier incentive program
- Increase effective use of Performance-based Logistics
- Reduce backlog of DCAA Audits without compromising effectiveness
- Expand programs to leverage industry’s IR&D

Reduce Unproductive Processes and Bureaucracy
- Reduce frequency of higher headquarters level reviews
- Re-emphasize AE, PEO and PM responsibility, authority, and accountability
- Reduce cycle times while ensuring sound investment decisions

Promote Effective Competition
- Emphasize competition strategies and creating and maintaining competitive environments
- Enforce open system architectures and effectively manage technical data rights
- Increase small business roles and opportunities
- Use the Technology Development phase for true risk reduction

Improve Tradecraft in Acquisition of Services
- Assign senior managers for acquisition of services
- Adopt uniform services market segmentation
- Improve requirements definition/prevent requirements creep
- Increase small business participation, including through more effective use of market research
- Strengthen contract management outside the normal acquisition chain – installations, etc.
- Expand use of requirements review boards and tripwires

Improve the Professionalism of the Total Acquisition Workforce
- Establish higher standards for key leadership positions
- Establish stronger professional qualification requirements for all acquisition specialties
- Increase the recognition of excellence in acquisition management
- Continue to increase the cost consciousness of the acquisition workforce – change the culture

For additional information on Better Buying Power 2.0: http://bbp.dau.mil/

Anti-Tamper is an export enabler for both Foreign Military Sales (FMS) and Direct Commercial Sales (DCS).
CPI Protection Throughout the Life Cycle

Balance CPI exposure – threat – consequence of loss
DoDI 5200.39 Critical Program Information (CPI) Protection Within the DoD

- Defines Critical Program Information (CPI) and establishes policy to identify it early in the technology development, acquisition, and sustainment process
- Defines and establishes Anti-Tamper as a protection measure for CPI

PPP Document Streamlining Memo & Outline and Defense Acquisition Guidebook (DAG) Chapter 13

- “Every acquisition program shall submit a PPP for Milestone Decision Authority review and approval at Milestone A and shall update the PPP at each subsequent milestone and the Full-Rate Production decision.”
- Provides a template and focal point all security activities on a program

AT Guidelines

- Initial CPI assessment and the associated preliminary AT protection requirements
- AT Concept Plan at Milestone A

Updates to DoDI 5200.39 and AT guidance are currently being worked in support of BBP v2.0
## Program Protection Plan

### Contents

#### Sections

1. Introduction
2. Program Protection Summary
3. **Critical Program Information (CPI) and Critical Functions**
   - Is there CPI?
   - How will it be protected?
4. Horizontal Protection
5. Threats, Vulnerabilities, and Countermeasures
6. Other System Security-Related Plans and Documents
7. Program Protection Risks
8. **Foreign Involvement and DEF**
   - Sales expectations?
   - Program a DEF candidate?
9. Processes for Management and Implementation of PPP
10. Processes for Monitoring and Reporting CPI Compromise
11. Program Protection Costs

#### Appendices

A. Security Classification Guide
B. Counterintelligence Support Plan
C. Criticality Analysis
D. **Anti-Tamper Plan (If Applicable)**
   - Sufficient for battlefield loss?
   - Sufficient for export?
E. Information Assurance Strategy
Implementation Considerations

- **CPI Determination**
  - Considering threat advancement, technology maturation, losses/CPI exposure, which change over time
  - Protecting CPI similarly across multiple programs and systems (horizontal protection)

- **Scaling the practice of AT**
  - Considering specialized technology, expertise, cost, and security

- **Business Processes**
  - Business case analysis; risk tradeoff methodology
  - Acquisition strategy and contractual mechanisms

- **Expertise and Resources across Government and Industry**
QUESTIONS?