



Comprehensive Program Protection Planning

Ms. Kristen Baldwin

Principal Deputy, Systems Engineering

Office of the Assistant Secretary of Defense, Research and Engineering

Defense Acquisition University

February 27, 2011

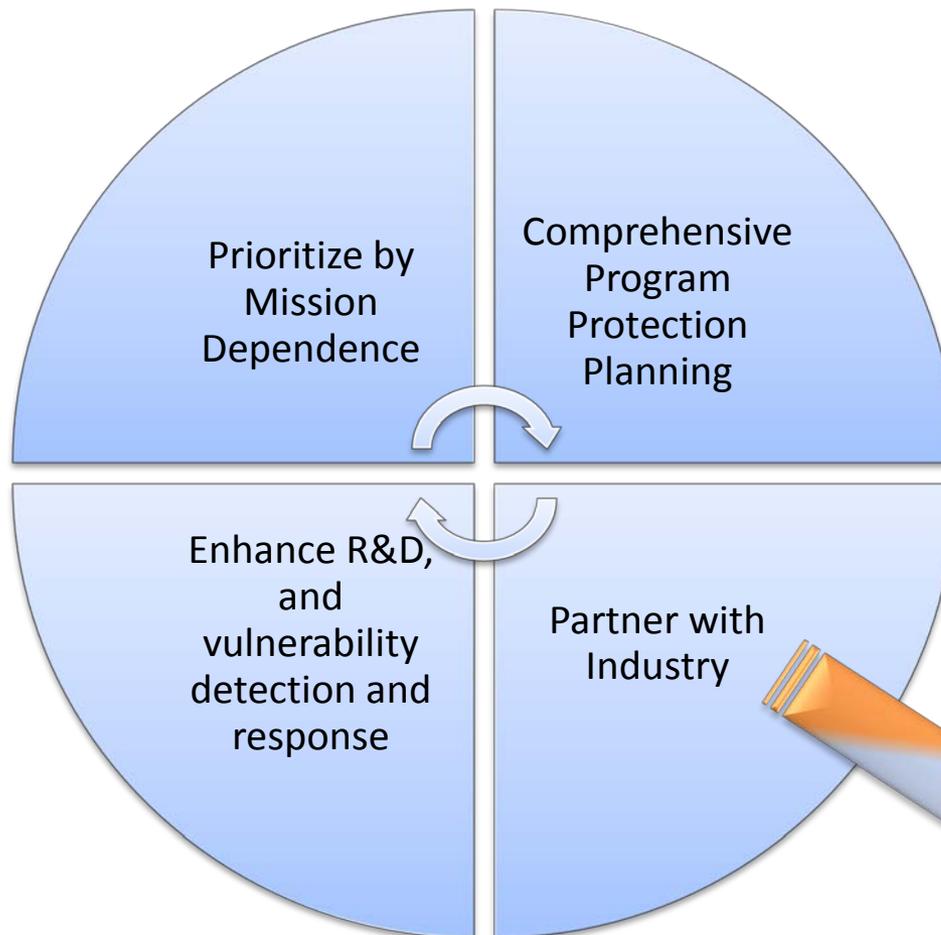


Trusted Defense Systems Strategy



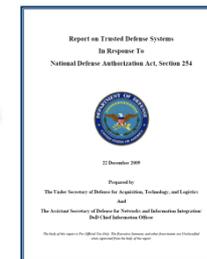
Drivers/Enablers

- National Cybersecurity Strategies
- Congressional Interest
- DoD Policy and Directives
- Globalization Challenges
- Increasing System Complexity



Delivering Trusted Systems

Report on Trusted Defense Systems



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



Trusted Defense Systems Strategy Basic Tenants



- **Prioritization:**
 - Focus security requirements on mission critical systems
 - Within systems, identify and protect critical components, technology, information
- **Comprehensive Program Protection Planning**
 - Early lifecycle identification of critical components
 - Provide PMs with intelligence analysis of supply chain risk
 - Protect critical components through trusted suppliers, or secure systems design
 - Assure systems through advanced vulnerability detection, test and evaluation
 - Manage counterfeit risk through sustainment
- **Partner with Industry**
 - Develop commercial standards for secure products
- **Enhance capability through R&D**
 - Leverage and enhance vulnerability detection tools and capabilities
 - Technology investment to advance secure software, hardware, and system design methods





Evolving Threat

- **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 (e.g., back doors, logic bombs, spyware)
 - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- **Traditional Consequences: Stolen critical data and technology**
- **Emerging Consequences: Exploitation of manufacturing and supply chain**
- **Either can result in corruption; denial of critical warfighting capability**



Today's acquisition environment drives the increased emphasis:

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



Program Protection Plan (PPP) Streamlining

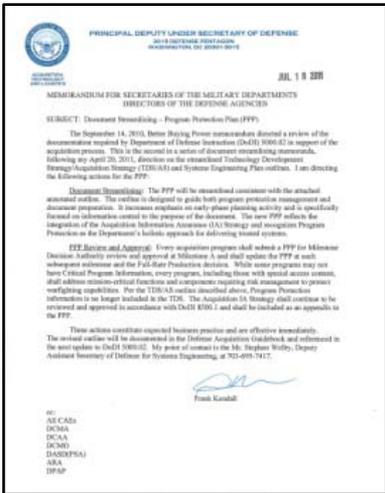


- **Vision: PPP is the consolidated security perspective for the program throughout the lifecycle**
- **Streamlined PPP content and format**
 - Moved to tables/bullets instead of essay paragraphs
 - Reduced boilerplate and front matter
 - Removed duplication across PPP annexes (Anti-Tamper Plan, Technology Assessment/Control Plan)
- **Coordinated disciplines to improve system security**
 - Supply Chain Risk Mitigation, Anti-Tamper, Security, Counterintelligence, Intelligence, System Security Engineering, Countering-Counterfeits, Information Assurance
 - Comprehensive PPP review/approval process
 - Coordination between USD(I), USD(AT&L), ASD(NII), Services, Anti-Tamper Executive Agent

*July 2011 PPP Outline and Guidance sets
expected business practice for all DoD programs*



New PPP Outline and Guidance



Signed by
Principal Deputy,
USD(AT&L) on
July 18, 2011

• What's in the Policy Memo?

- *“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.”*
- Existing acquisition Information Assurance Strategy
 - Appendix to PPP: Subject to a page count limit
- Expected business practice, effective immediately, and reflected in upcoming DoDI 5000.02 and DAG updates

• What's in the Outline and Guidance?

- 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
- Similar approach as TDS/AS and SEP Outline and Guidance

The PPP is the Single Focal Point for All Security Activities on the Program



What Are We Protecting?

Program Protection Planning

DODI 5000.02 Update

DoDI 5200.39
Change 1, dated Dec 10

DTM 09-016

DoDI 5200.39
DTM 09-016

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

Note: Program Protection Planning Includes DoDI 8500 series



System Security Engineering (SSE) Throughout the Full Lifecycle



- **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

MIL-HDBK-1785: System Security Engineering Program Management Requirements

- **Use criticality analyses, vulnerability assessment, threats assessment and cost benefit risk trade-off to select and refine countermeasures**

- **Pre-Milestone A:** Evaluate mission threads, identify system functions, and analyze notional system architectures to identify mission critical functions, potential components and countermeasures. Incorporate countermeasures into RFP
- **Pre-Milestone B:** Refine critical function list, identify critical system components (hardware, software, and firmware) and secure design countermeasures. Incorporate countermeasures into RFP and repeat trade-off analysis. Plan security verification and penetration testing.
- **Pre-Milestone C:** Refine list of critical system components and countermeasures. Update trade-off analysis wrt physical design baseline to update countermeasures as necessary. Begin security and penetration testing.
- **Pre-FRP Decision or FDD Review:** Repeat analysis and assessments to update risks and trade-off analysis to incorporate security verification and penetration testing results. Adjust countermeasure plan as required. Develop program protection Life Cycle Sustainment Plan.
- **Operations & Sustainment:** Review and maintain list of critical system components Whenever there is a technology refresh perform analysis and assessments and to update countermeasures. Periodically reassess vulnerabilities.



Risk Assessment Methodology



Input Analysis Results:

Criticality Analysis Results

| Mission | Critical Functions | Logic-Bearing Components (HW, SW, Firmware) | System Impact (I, II, III, IV) | Rationale |
|-----------|--------------------|---|--------------------------------|-------------|
| Mission 1 | CF 1 | Processor X | II | Redundancy |
| | CF 2 | SW Module Y | I | Performance |
| Mission 2 | CF 3 | SW Algorithm A | II | Accuracy |
| | CF 4 | FPGA 123 | I | Performance |

Vulnerability Assessment Results

| Critical Components (HW, SW, Firmware) | Identified Vulnerabilities | Exploitability | System Impact (I, II, III, IV) | Exposure |
|--|--|-------------------------------|--------------------------------|------------------------------|
| Processor X | Vulnerability 1 Vulnerability 4 | Low Medium | II | Low Low |
| SW Module Y | Vulnerability 1 Vulnerability 2 Vulnerability 3 Vulnerability 6 | High Low Medium High | I | High Low Medium Low |
| SW Algorithm A | None | Very Low | II | Very Low |
| FPGA 123 | Vulnerability 1 Vulnerability 23 | Low Low | I | High High |

Threat Analysis Results

| Supplier | Critical Components (HW, SW, Firmware) | TAC Findings |
|------------|--|-----------------------------|
| Supplier 1 | Processor X | Potential Foreign Influence |
| | FPGA 123 | Potential Foreign Influence |
| Supplier 2 | SW Algorithm A | Cleared Personnel |
| | SW Module Y | Cleared Personnel |

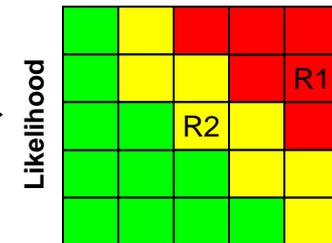
Risk Mitigation and Countermeasure Options

| Consequence of Losing Mission Capability |
|--|
| Very High |
| High |
| Moderate |
| Low |
| Very Low |

| Likelihood of Losing Mission Capability |
|---|
| Near Certainty (VH) |
| Highly Likely (H) |
| Likely (M) |
| Low Likelihood (L) |
| Not Likely (VL) |

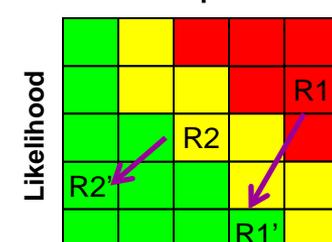
Initial Risk Posture

Consequence



Risk Mitigation Decisions

Consequence





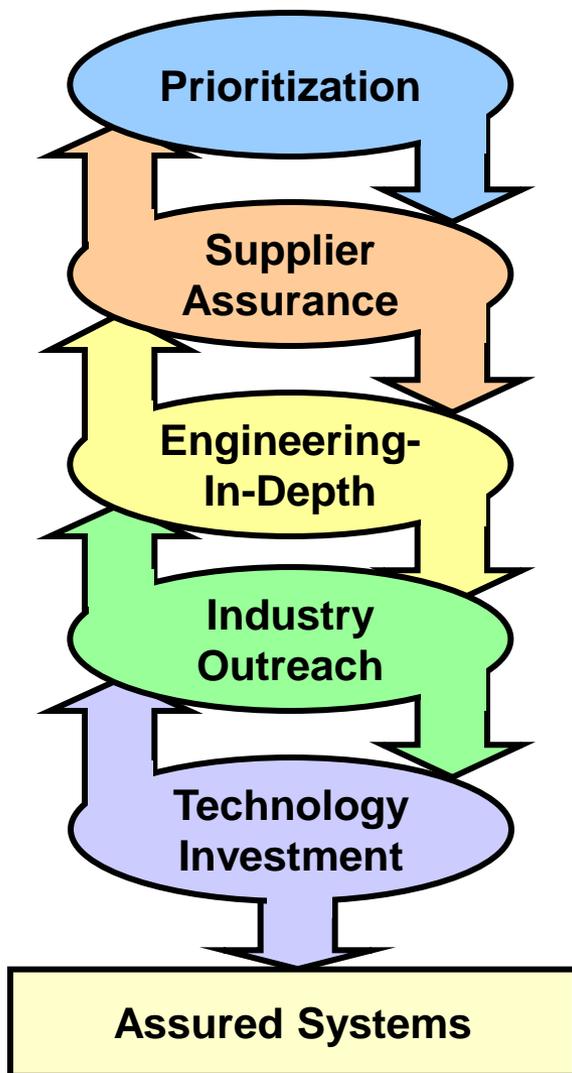
In Summary



- **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, Intelligence, Engineering, Industry, Research 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



Vision of Success



- The requirement for assurance is allocated among the right systems and their critical components
- DoD understands its supply chain risks
- DoD systems are designed and sustained at a known level of assurance
- Commercial sector shares ownership and builds assured products
- Technology investment transforms the ability to detect and mitigate system vulnerabilities

*Reference: DoD System Assurance CONOPS, 2004



Questions?