



Comprehensive Program Protection Planning

Paul R. Popick

Aerospace Corporation

Paul.Popick.ctr@osd.mil/ 703 681-6563

Phoenix Challenge Conference

April 26, 2012

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE APR 2012		2. REPORT TYPE		3. DATES COVERED 00-00-2012 to 00-00-2012	
4. TITLE AND SUBTITLE Comprehensive Program Protection Planning				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Aerospace Corporation,2310 E. El Segundo Blvd,Los Angeles,CA,90245				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES Presented at Phoenix Challenge Conference, at Lawrence Livermore National Laboratory, Livermore, CA. April 24-26, 2012,Government or Federal Purpose Rights License					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 12	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

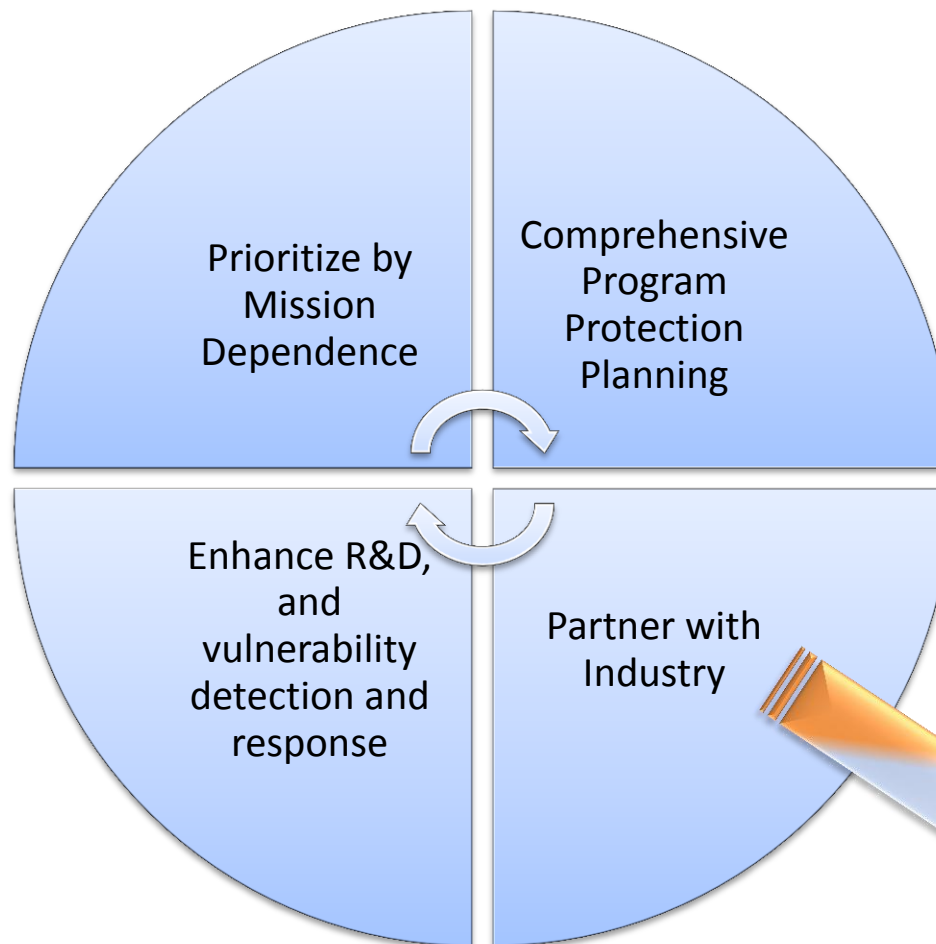


Trusted Defense Systems Strategy



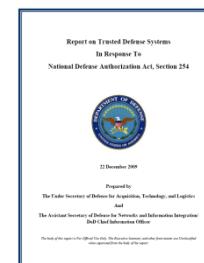
Drivers/Enablers

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



Delivering Trusted Systems

Report on Trusted Defense Systems



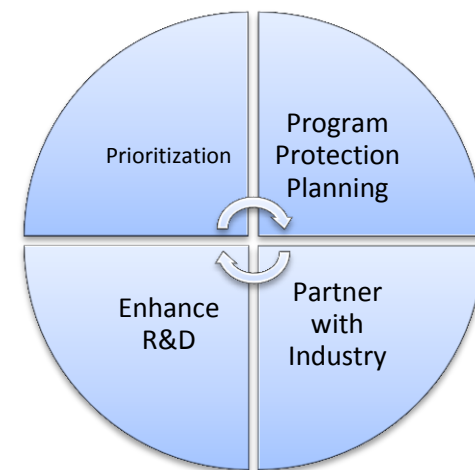
USD(AT&L)
ASD(NII)/DoD CIO



Trusted Defense Systems Strategy Basic Tenets



- **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 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





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:

<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 Policy Framework



DoDI 5000.02 Enclosure 14: Program Protection

- PPP for every program at every milestone
- Identify CPI and critical functions/components
- Use Intelligence/Counterintelligence support to identify threats
- Use cost-effective countermeasures to mitigate risk
- Include IA Strategy with PPP
- Incorporate in T&E to ensure implementation

Signed

Draft

DoDI 5200.39 Protection of CPI

Focus: Protect **leading-edge research and technology** from battlefield loss and unauthorized transfer

Countermeasures: Anti-Tamper, Classification, Export Control, Security, Foreign Disclosure, and CI activities

DoDI 5200.mm Trusted Systems and Networks

Focus: Protect **mission-critical functionality** from compromise through system design or supply chain exploit

Countermeasures: Supply Chain Risk Management (SCRM), Software Assurance (SwA), System Security Engineering (SSE)

DoDD 8500.01 Information Assurance

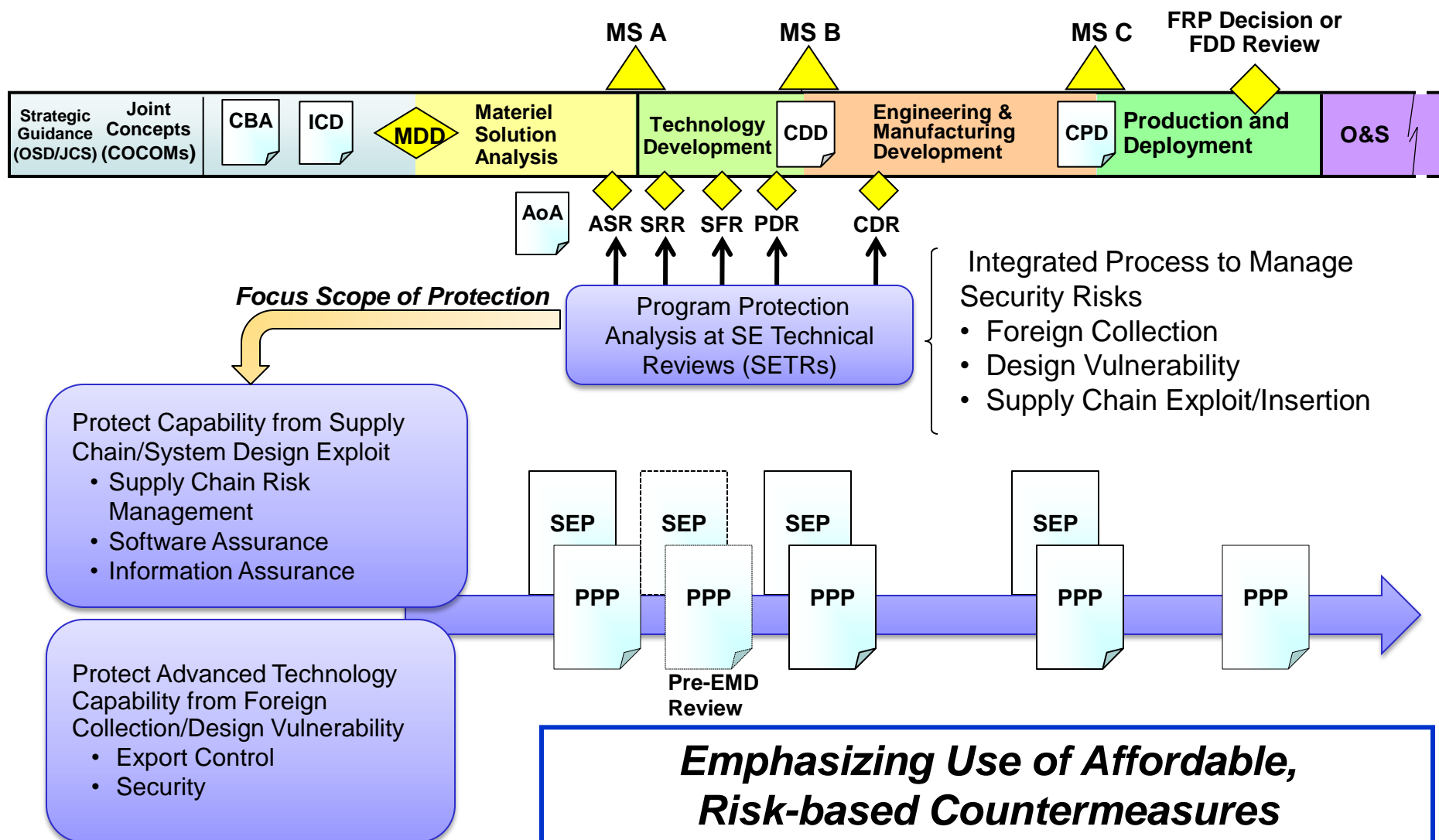
Focus: Assure confidentiality, integrity, and availability of **information** and information systems

Countermeasures: IA Controls (technical, process, management, awareness & training, etc.)

Complementary framework enables comprehensive Program Protection



Program Protection Embedded in Technical Reviews





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

Supplier Risk Analysis Results

Supplier	Critical Components (HW, SW, Firmware)	Analysis Findings
Supplier 1	Processor X	Supplier Risk
	FPGA 123	Supplier Risk
Supplier 2	SW Algorithm A	Cleared Personnel
	SW Module Y	Cleared Personnel

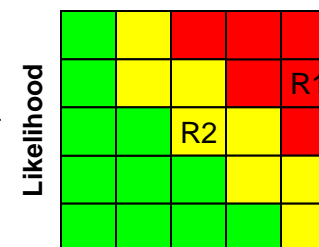
Risk Mitigation and Countermeasure Options

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)

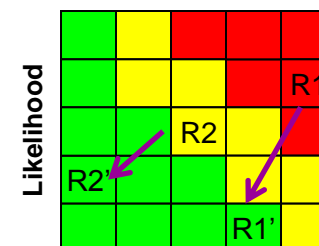
Initial Risk Posture

Consequence



Risk Mitigation Decisions

Consequence





International Community System Assurance Activities



- **ISO/IEC 15026 – System and Software Engineering – Systems and Software Assurance**
 - Establishes common assurance concepts, vocabulary, integrity levels and lifecycle
- **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)**
 - Systems Security Engineering (SSE) working group established to develop SSE updates to INCOSE SE Handbook
- **The Open Group (TOG)**
 - The Open Trusted Technology Provider Framework (O-TTPF) - open standard that codifies best practices across the entire lifecycle covering:
 - Product Development
 - Secure Engineering
 - Supply Chain Integrity
 - <http://www.opengroup.org/ogttf/>



System Security Engineering (SSE) Research Activities



DoD is leveraging the Systems Engineering Research Center (SERC) —a DoD University Affiliated Research Center led by Stevens Institute with over 20 collaborating university partners—to advance SSE

- **Published the SSE Research Roadmap in August 2010**



- Outlines approach for advancing SSE definitions, metrics, frameworks, and human capital through coordinated research modules
- Captures input from 50+ industry, academia, and government experts

- **Conduct follow-on research into “System Aware” Security**



- Prototype secure design patterns and study system performance impacts
 - Physical and virtual configuration hopping
 - Diverse redundancy of components
 - Voting mechanisms
- Develop scoring model for evaluating efficacy of security solutions
 - Identify contribution of individual security services
 - Determine effectiveness of security services within a security architecture
 - Evaluate cost and collateral impacts



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



Questions?