Cyber Resiliency of Defense Systems

Ms. Kristen Baldwin

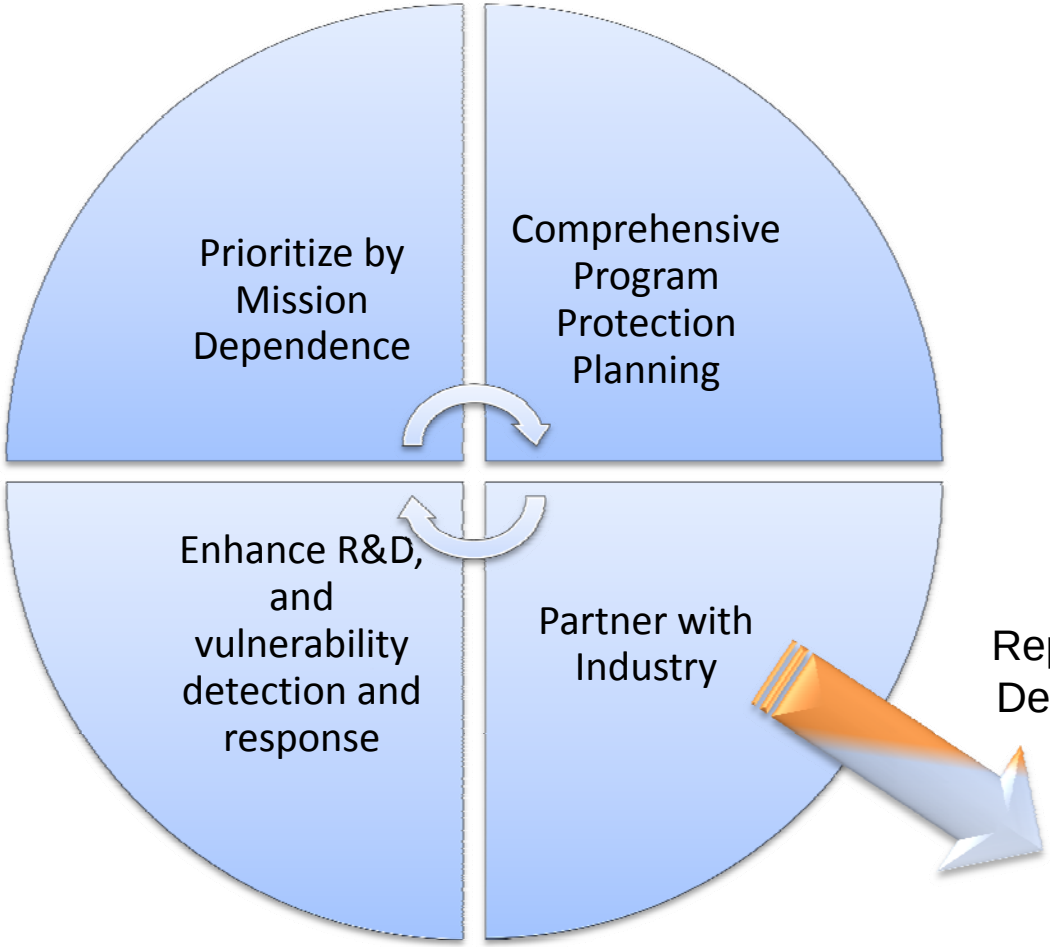
Principal Deputy, Systems Engineering
Office of the Assistant Secretary of Defense, Research and Engineering

Women In Defense National Fall Conference
October 19, 2011

Trusted Defense Systems Strategy

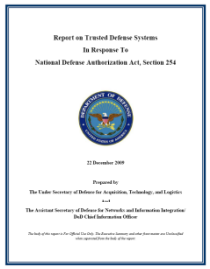
Drivers/Enablers

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



Delivering Trusted Systems

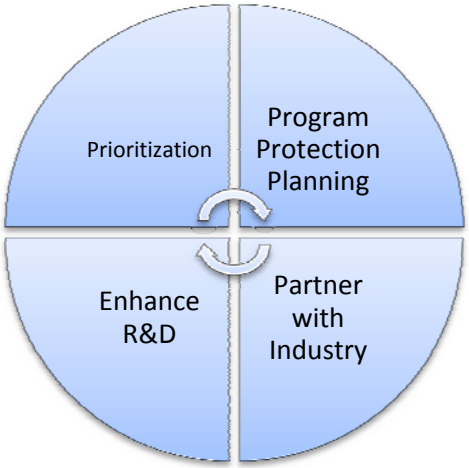
Report on Trusted Defense Systems



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



Threats

- ***Threats*: Nation-state, terrorist, criminal, rogue developer who:**
  - Gain control of systems through supply chain opportunities
  - Exploit vulnerabilities remotely
- ***Vulnerabilities*: All systems, networks, applications**
  - Intentionally implanted logic (e.g., back doors, logic bombs, spyware)
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- ***Consequences*: Stolen critical data & technology; corruption, denial of critical warfighting capability**

Today's acquisition environment drives the increased emphasis:

Then		Now
Standalone systems	**>>>**	**Networked systems**
Some software functions	**>>>**	**Software-intensive**
Known supply base	**>>>**	**Prime Integrator, hundreds of suppliers**

What We Are Protecting

Program Protection Planning

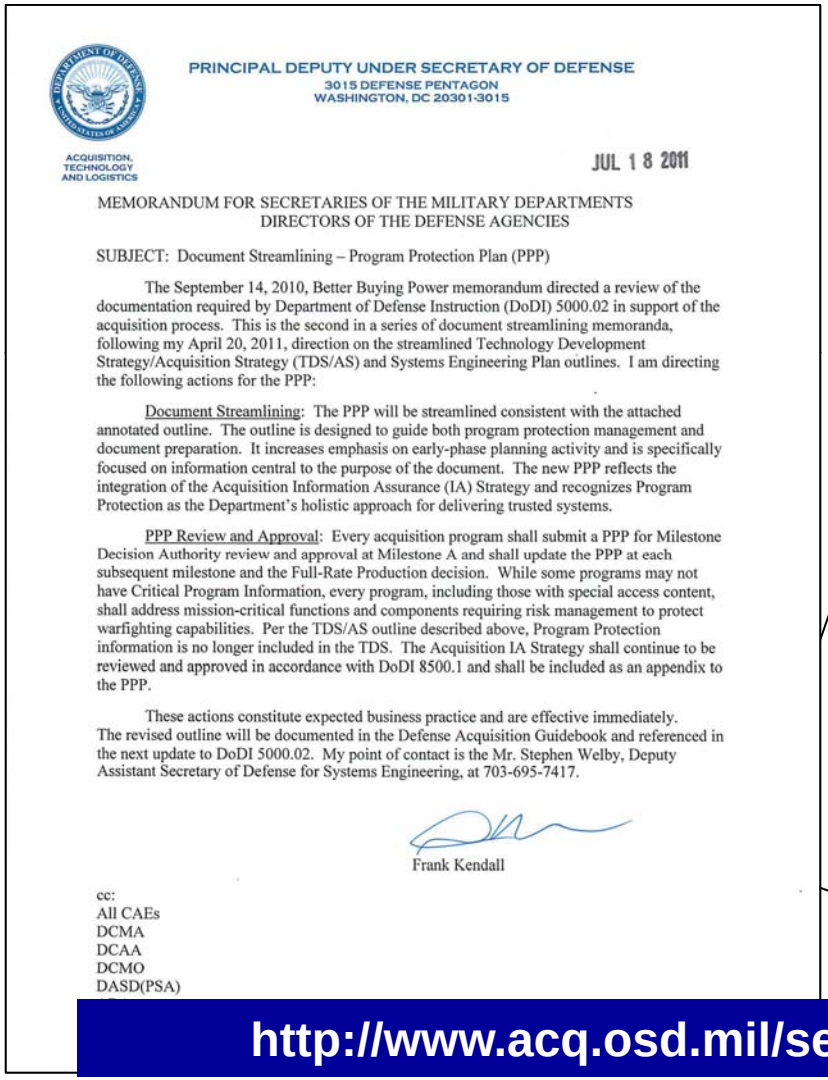
DoDI 5000.02 Update

DoDI 5200.39 Change 1, dtd Dec 10	DTM 09-016 DoDI 5200.cc, TBD	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:** TTRA, M/D-CITA **Countermeasures:** AT, Classification, Export Controls, Security, etc. **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:** Various **Threat Assessment:** Various **Countermeasures:** Information Assurance, Classification, Export Controls, Security, etc. **Focus:** Keep critical information from getting out by protecting data

Protecting Warfighting Capability Throughout the Lifecycle

* Program Protection Planning Includes DoDI 8500 series

Program Protection Plan Outline and Guidance as "Expected Business Practice"



PRINCIPAL DEPUTY UNDER SECRETARY OF DEFENSE
3015 DEFENSE PENTAGON
WASHINGTON, DC 20301-3015

ACQUISITION, TECHNOLOGY AND LOGISTICS

JUL 18 2011

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Document Streamlining – Program Protection Plan (PPP)

The September 14, 2010, Better Buying Power memorandum directed a review of the documentation required by Department of Defense Instruction (DoDI) 5000.02 in support of the acquisition process. This is the second in a series of document streamlining memoranda, following my April 20, 2011, direction on the streamlined Technology Development Strategy/Acquisition Strategy (TDS/AS) and Systems Engineering Plan outlines. I am directing the following actions for the PPP:

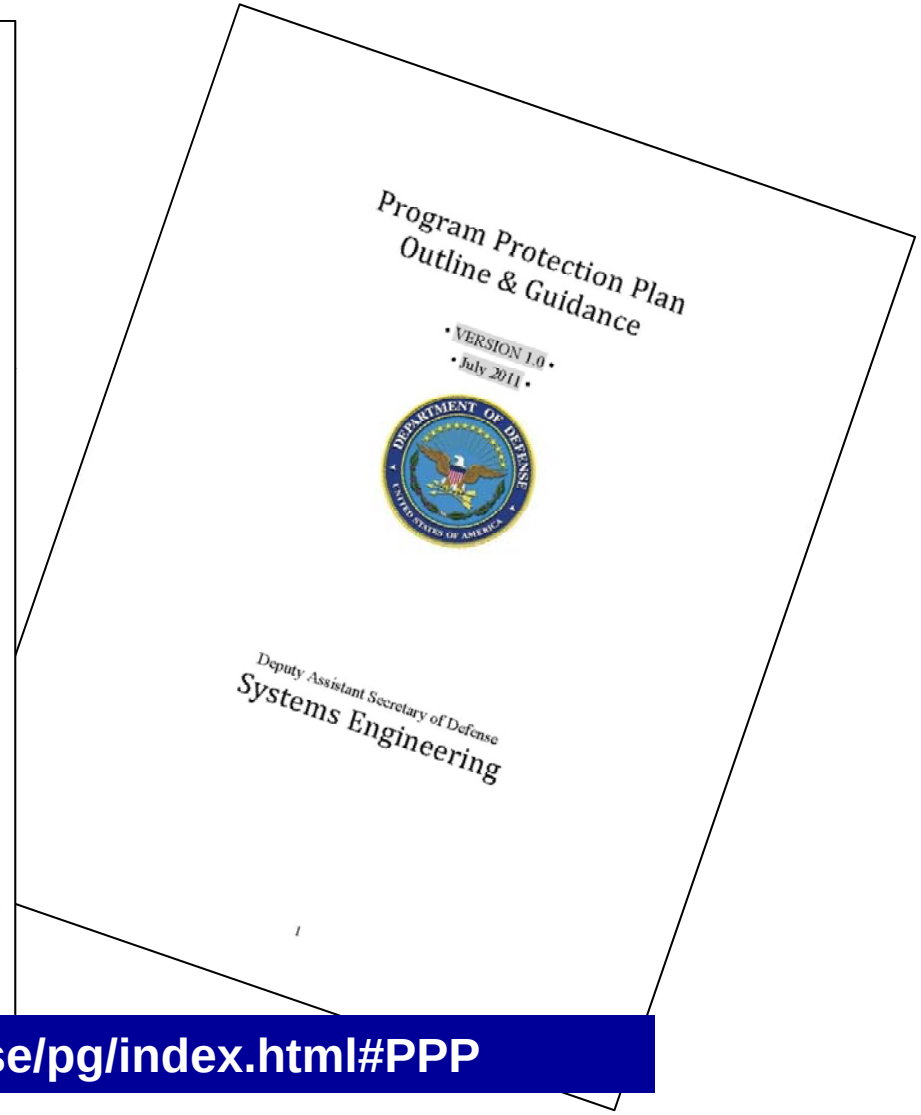
Document Streamlining: The PPP will be streamlined consistent with the attached annotated outline. The outline is designed to guide both program protection management and document preparation. It increases emphasis on early-phase planning activity and is specifically focused on information central to the purpose of the document. The new PPP reflects the integration of the Acquisition Information Assurance (IA) Strategy and recognizes Program Protection as the Department's holistic approach for delivering trusted systems.

PPP Review and Approval: 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. While some programs may not have Critical Program Information, every program, including those with special access content, shall address mission-critical functions and components requiring risk management to protect warfighting capabilities. Per the TDS/AS outline described above, Program Protection information is no longer included in the TDS. The Acquisition IA Strategy shall continue to be reviewed and approved in accordance with DoDI 8500.1 and shall be included as an appendix to the PPP.

These actions constitute expected business practice and are effective immediately. The revised outline will be documented in the Defense Acquisition Guidebook and referenced in the next update to DoDI 5000.02. My point of contact is the Mr. Stephen Welby, Deputy Assistant Secretary of Defense for Systems Engineering, at 703-695-7417.

Frank Kendall

cc:
All CAEs
DCMA
DCAA
DCMO
DASD(PSA)



Program Protection Plan
Outline & Guidance

• VERSION 1.0 •
• July 2011 •

Deputy Assistant Secretary of Defense
Systems Engineering

1

http://www.acq.osd.mil/se/pg/index.html#PPP

Program Protection Plan (PPP) Streamlining

- **<u>Vision</u>: 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

Systems Security Engineering (SSE): Early Engineering Emphasis

- **Identify components that need protection**
  - Perform criticality analysis based on mission context and system function
    - Evaluate CONOPS, threat information, notional system architecture to identify critical components (hardware, software and firmware)
    - Identify rationale for inclusion or exclusion from candidate CPI list
  - Perform trade-offs of design concepts and potential countermeasures to minimize vulnerabilities, weaknesses, and implementation costs
- **Establish Systems Security Engineering Criteria**
  - Ensure preferred concept has preliminary level security requirements derived from candidate CPI countermeasures
  - Ensure system security is addressed as part of Systems Engineering Technical Reviews
- **We have begun to apply these practices with major acquisition programs**
  - In support of risk-based Program Protection Plan development
  - In preparation for MS B and MS C Defense Acquisition Board 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	Exploit-ability	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

Supply Chain Threat Analysis Results

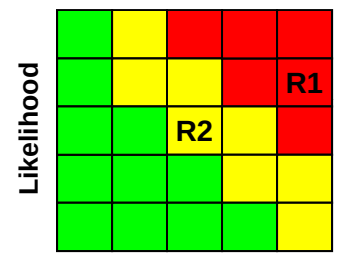
Supplier	Critical Components (HW, SW, Firmware)	TAC Findings
Supplier 1	Processor X	Potential Foreign Influence
	FPGA 123	Potential Foreign Influence
Supplier 2	SW Algorithm A	Cleared Personnel
	SW Module Y	Cleared Personnel

Risk Mitigation and Countermeasure Options

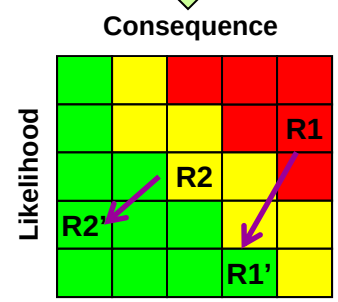
Consequence of Losing Mission Capability
Very High
High
Moderate
Low
Very Low

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

Initial Risk Posture



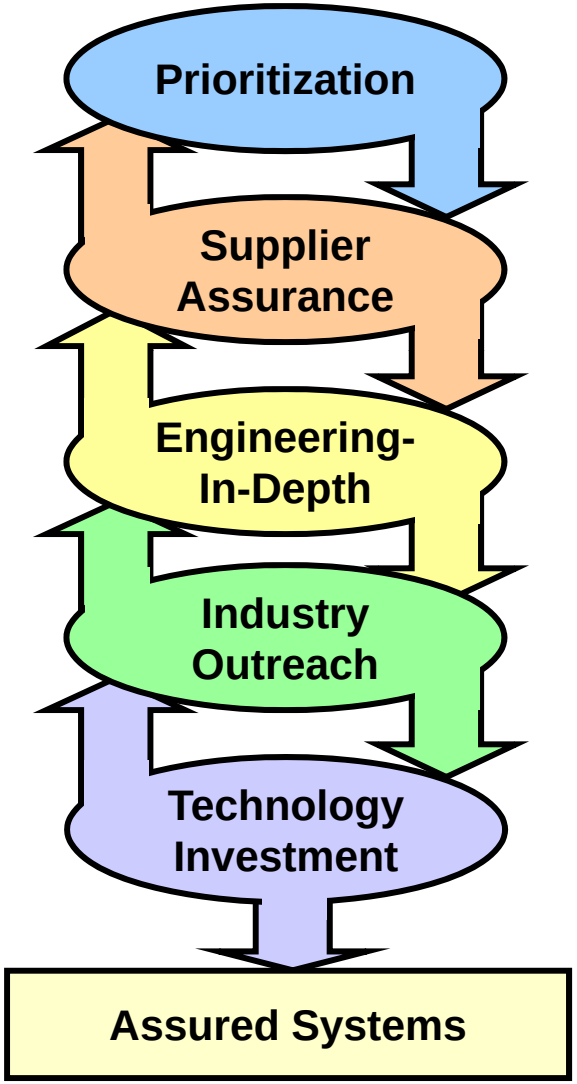
Risk Mitigation Decisions



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?

Criticality Analysis Methodology

Inputs:

- ICD
- CDD
- Concept of Operations
- Concept of Employment
- Software development processes
- Sources and performance experience of key data handling components
- System architecture down to component level
- Vulnerabilities
- Verification plans
- WBS
- Etc.

Leverage existing mission assurance analysis, including flight & safety critical

Identify and Group Mission Threads by Priority

↓

Identify Critical Functions Assign Criticality Levels

↓

Map Threads and Functions to Subsystems and Components

↓

Identify Critical Suppliers

Criticality Levels

Level I:	Total Mission Failure
Level II:	Significant/Unacceptable Degradation
Level III:	Partial/Acceptable Degradation
Level IV:	Negligible

Outputs:

- Table of Level I & II Critical Functions and Components
- TAC Requests for Information

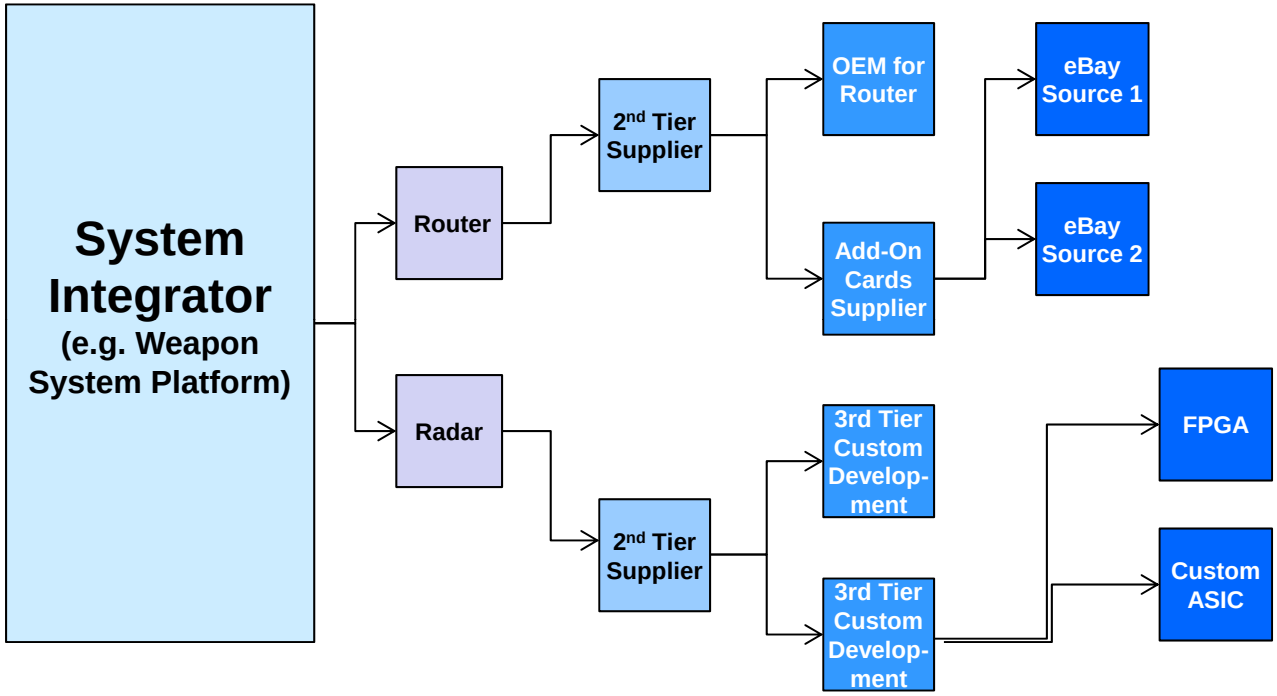
Vulnerability Assessment Methodology

- **Inputs**
  - System architecture
  - Critical functions and components
  - Design, development, integration and test processes
  - Manufacturing processes
  - Software development processes
  - Update, configuration, and maintenance processes

- **Processes**
  - Review all stages of the inputs to identify access opportunities for introducing and exploiting vulnerabilities

- **Outputs**
  - Risks due to vulnerabilities of the system, critical functions, and critical components
  - Countermeasure and mitigation suggestions

Tiered Supply Chain
(Notional Example)



Supplier Threat can reside several layers down from System Integrator

How is it shipped?
How is it verified and validated ?
How is it physically protected?
Do you execute a Blind Buy?
…

Manage Risks

Criticality
Schedule
Cost

1st Tier Supplier
2nd Tier Supplier
3rd Tier Supplier
4th Tier Supplier

Key Elements of the PPP

Key Sections	Rationale
3.0 CPI and Critical Components (CC) – Documents output of Research & Tech. Protect and Criticality Analysis – Distinguishes between inherited and organic elements	**Focus protection on critical technology, information, and components**
4.0 Horizontal Protection – Assessment of similar CPI on other DoD programs, ASDB status	**Protect technologies across the DoD**
5.0 Threats – Identifies foreign collection, supply chain, and battlefield threats	**Acknowledge advanced, persistent threat**
6.0 Vulnerabilities and Countermeasures – Documents assessment of vulnerability to threats and mitigating actions	**Assess weaknesses to documented threats and use risk-based mitigations**
7.0 Other Plans – Pointers to related documents (CI Support Plan, TEMP, etc.)	**Reference, not duplicate, key documents**
8.0 Residual Risk Assessment – Document unmitigated risks to CPI and CC compromise	**Document risks program is assuming**
9.0 Foreign Involvement – Identify known and potential co-development, foreign military sales, and direct commercial sales	**Drive export realism and prepare for export-specific countermeasures early**
10.0 Processes for PM Oversight & Implementation	**PM Resources and Implementation Reviews**
11.0 Processes for Monitoring & Reporting Loss of CPI and CC – Monitor open source and intelligence sources for loss	**Assess effectiveness of implemented countermeasures**
12.0 Costs – Estimate of implementation costs for CPI and CC protection	**Support cost/benefit assessment of risk mitigations**

The PPP contains the information a PM needs to effectively secure the system