Comprehensive Program Protection Planning

E. Kenneth Hong Fong

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

14th Annual NDIA Systems Engineering Conference
San Diego, CA | October 25, 2011

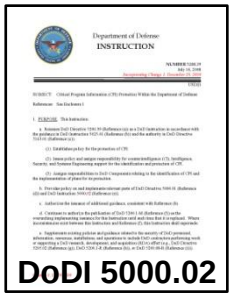
Threats

- ***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 and technology; corruption, denial of critical warfighting capability**

Today's acquisition environment drives the increased emphasis:

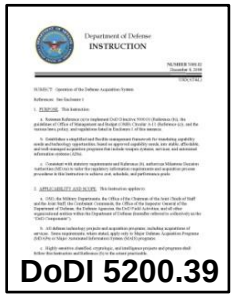
Then		Now
Standalone systems	>>>	Networked systems
Some software functions	>>>	Software-intensive
Known supply base	>>>	Prime Integrator, hundreds of suppliers

Existing Policy


Department of Defense
INSTRUCTION

DoDI 5000.02

- **DoDI 5000.02, dtd Dec 2008**
  - *Operation of Defense Acquisition System*
  - Regulatory Requirement for Program Protection Plan at MS B/C
  - References DoDI 5200.39


Department of Defense
INSTRUCTION

DoDI 5200.39

- **DoDI 5200.39, dtd Dec 2010**
  - *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
    - Technology, information, elements of components

DTM 09-016

- **Directive-Type Memorandum (DTM) 09-016, Sep 2010**
  - *Supply Chain Risk Management to Improve the Integrity of Components Used in DoD Systems*
  - Establishes policy and defense-in-breadth strategy for managing Supply Chain Risk to information and communications technology

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 1 8 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:

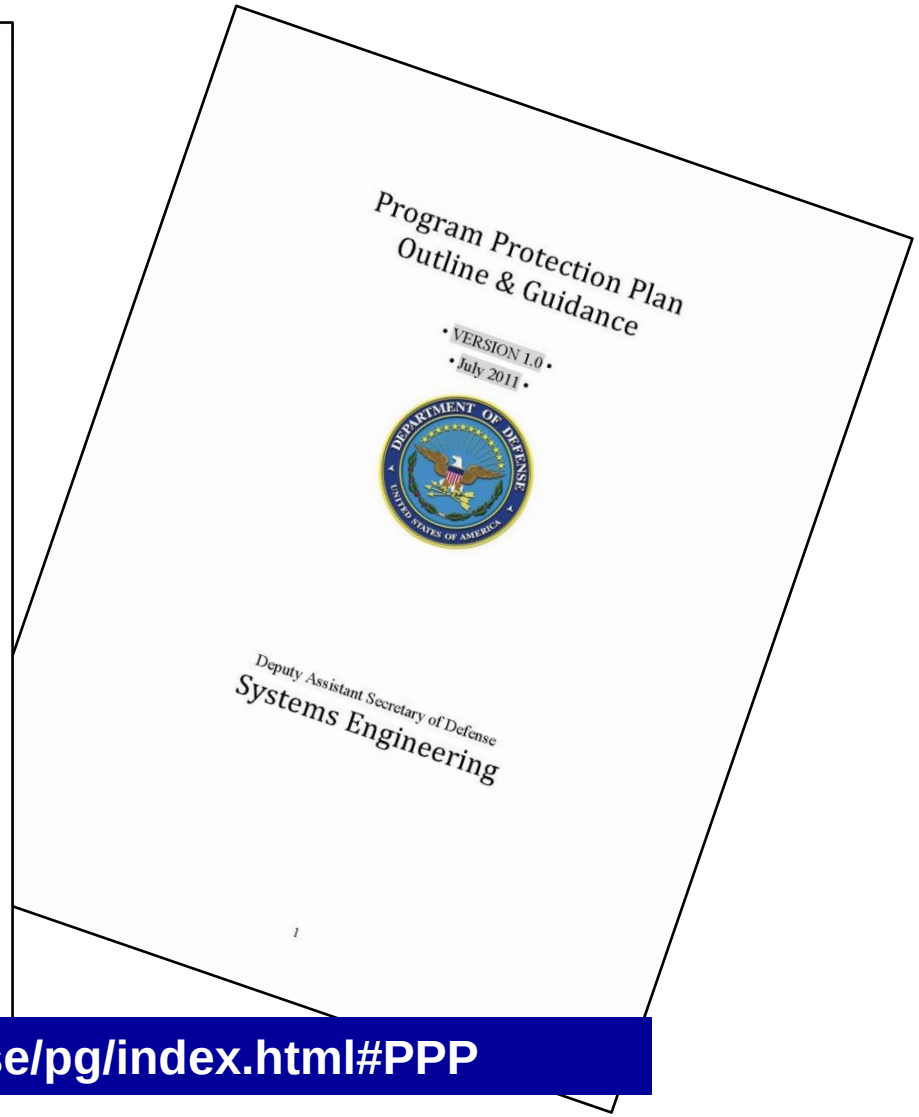
Document Streamlining: The PPP will be streamlined consistent with the attached annotated outline. The outline is designed to guide both program protection management and document preparation. It increases emphasis on early-phase planning activity and is specifically focused on information central to 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)

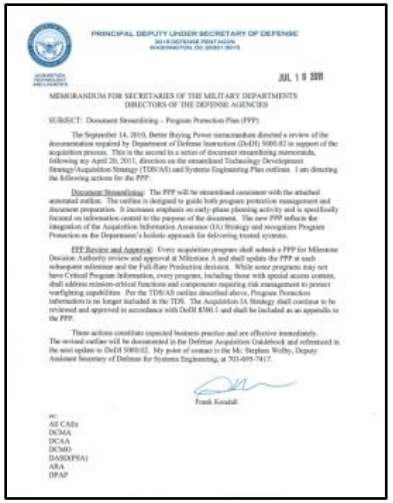


http://www.acq.osd.mil/se/pg/index.html#PPP

PPP Outline and Guidance

- **What's in the outline**
  - 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

- **What's in the policy memo**
  - Every program shall submit a PPP at every milestone and the Full Rate Production decision
  - Acquisition IA Strategy shall be included as PPP appendix
  - Expected business practice, effective immediately and reflected in upcoming DoDI 5000.02 and DAG updates



PRINCIPAL DEPUTY UNDER SECRETARY OF DEFENSE

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:
AE CAEs
DCMA
DCAA
DCMO
DASD(PSA)
ARA
DPAP

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

The PPP is the single focal point for all security activities on the program

Current Policy Initiatives

- **DoDI 5000.02 – Program Protection Enclosure**
  - Purpose: Umbrella program protection direction to all programs. Covers technology protection and trusted systems.
  - Status: Coordinated with Service stakeholders, awaiting release of full 5000.02 for comment
- **DoDI 5200.mm – Trusted Systems and Networks**
  - Purpose: Establish policy and responsibilities for the identification and protection of critical functions through Program Protection. Converts SCRM DTM into lasting policy. "Parallel" to DoDI 5200.39.
  - Status: In formal coordination
- **Defense Acquisition Guidebook – Program Protection Chapter**
  - Purpose: Provide program protection guidance, expectations following the organization of the signed PPP Outline.
  - Status: "Fact of Life" edits provided Sept. 14. A second edit will occur after the next DoDI 5000.02 is signed.

What We Are Protecting

Program Protection Planning

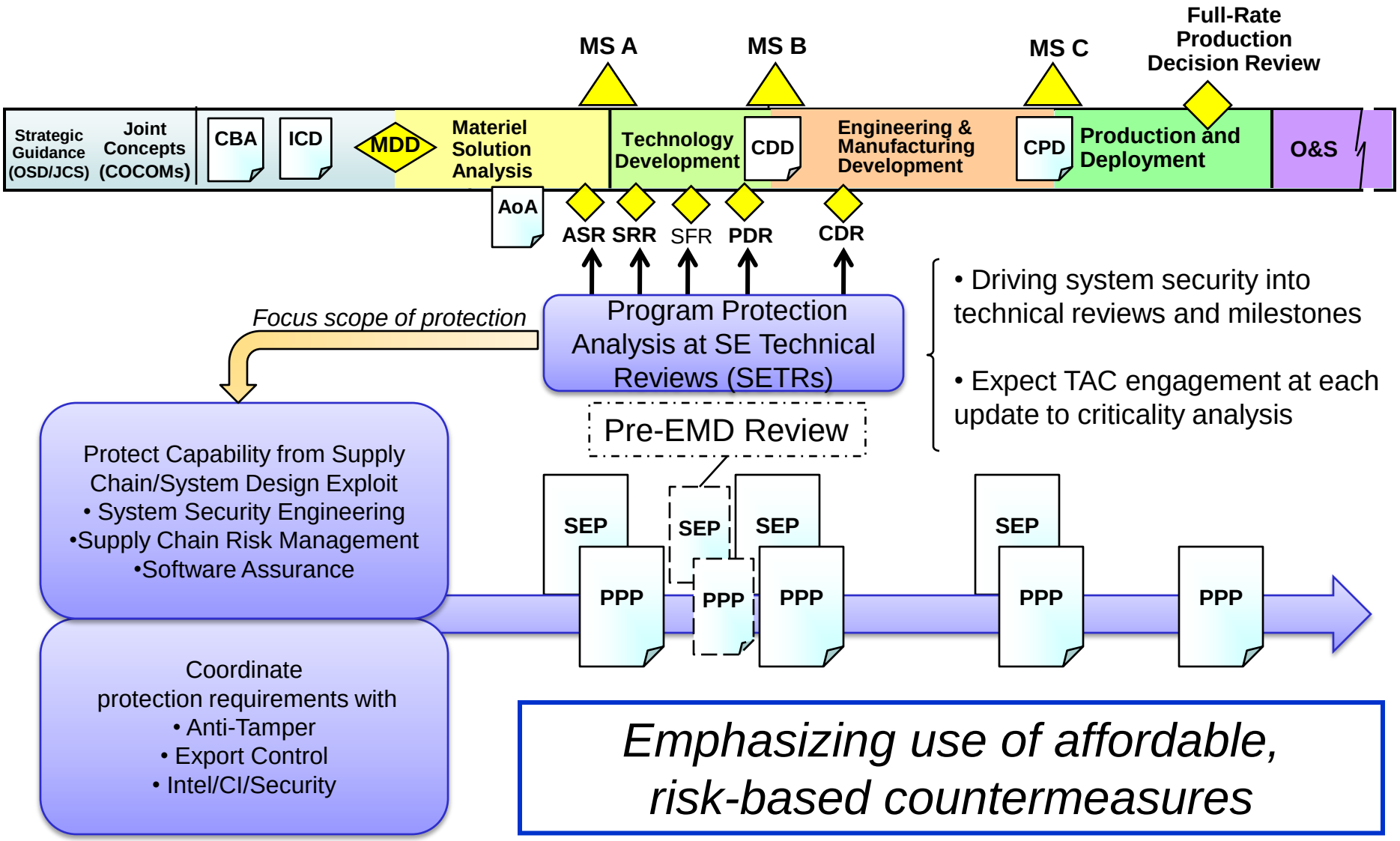
DoDI 5000.02 Update

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	**What:** Mission-critical elements and components	**What:** Information about applications, processes, capabilities and end-items
Who Identifies: Technologists, System Engineers	**Who Identifies:** System Engineers, Logisticians	**Who Identifies:** All
ID Process: CPI Identification	**ID Process:** Criticality Analysis	**ID Process:** Various
Threat Assessment: TTRA, M/D-CITA	**Threat Assessment:** DIA SCRM TAC	**Threat Assessment:** Various
Countermeasures: AT, Classification, Export Controls, Security, etc.	**Countermeasures**: SCRM, SSE, Anti-counterfeits, software assurance, Trusted Foundry, etc.	**Countermeasures:** Information Assurance, Classification, Export Controls, Security, etc.
Focus: "Keep secret stuff in" by protecting any form of technology	**Focus:** "Keep malicious stuff out" by protecting key mission components	**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 Embedded in SETRs



Criticality Analysis Methodology

Criticality Analysis

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.

Identify and Group Mission Threads by Priority

↓

Identify Critical Functions Assign Criticality Levels

↓

Map Threads and Functions to Subsystems and Components

↓

Identify Critical Suppliers

→

Outputs:

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

Leverage existing mission assurance analysis, including flight & safety critical

Criticality Levels

Level I: Total Mission Failure

Level II: Significant/Unacceptable Degradation

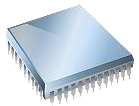
Level III: Partial/Acceptable Degradation

Level IV: Negligible

Vulnerability Assessment Considerations

Vulnerability Assessment

❑ Where and Under What Conditions was the System Designed?



- Who made significant system-wide design decisions?
- Who has had access to design information?
- How are requirements and specifications for critical components communicated to suppliers?
- How much do suppliers know about how critical their products are to the overall system?

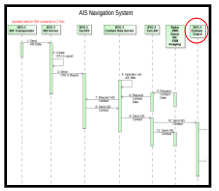
❑ Where and Under What Conditions were Critical Components Developed?

- For custom components, who made significant design decisions?
- Who has had access to design information?
- Where are critical components fabricated or manufactured?
- Who has had access to fabrication or manufacturing processes?
- What testing of critical components has been conducted? How and where?
- How are critical components shipped?
- How has custody of critical components been managed?

CONOPS

System Requirements

Data Flow Diagrams

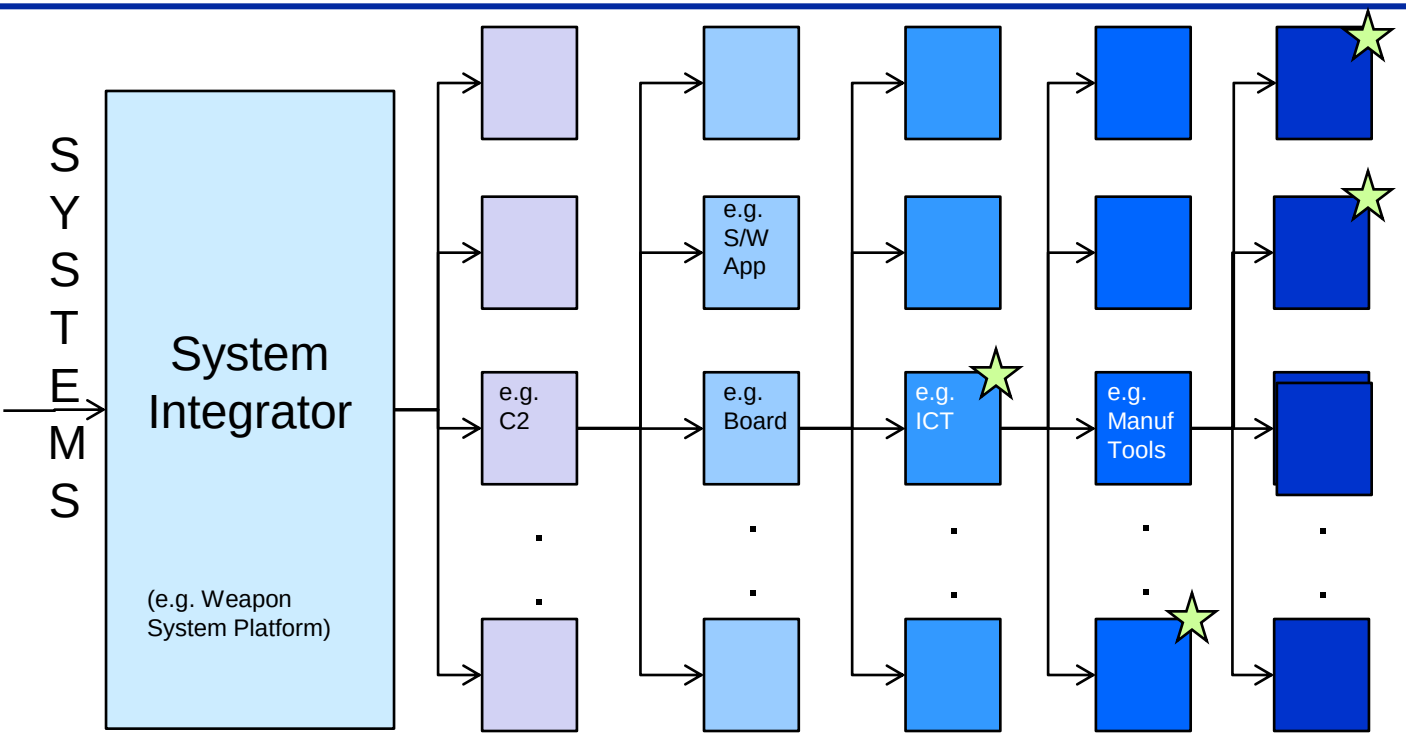


❑ How and Where are Components Assembled and Integrated into Completed Systems?

- What final system testing is conducted?

Assessing Vulnerability of Critical Components

Tiered Supply Chain Problem



- Critical components may be sourced from deep within contract stack
- PMs depend on TAC assessments of nth-tier suppliers
- Vulnerability assessments for critical components ask key questions

1st Tier Supplier
2nd Tier Supplier
3rd Tier Supplier
4th Tier Supplier
5th Tier Supplier
TAC Assessment

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?
How is it shipped?
Do you execute a Blind Buy?

Manage Risks

Criticality
Schedule
Cost

Software Assurance Methods Vulnerability Assessment

Vulnerability Assessment

Table 5.3-5-5: Application of Software Assurance Countermeasures (sample)

Development Process								
Software (CPI, critical function components, other software)	**Static Analysis p/a**	**Design Inspect**	**Code Inspect p/a**	**CVE p/a**	**CAPEC p/a**	**CWE p/a**	**Pen Test**	**Test Coverage p/a**
Developmental CPI SW	100/80%	Two Levels	100/80	100/60	100/60	100/60	Yes	75/50%
Developmental Critical Function SW	100/80%	Two Levels	100/80	100/70	100/70	100/70	Yes	75/50%
Other Developmental SW	none	One level	100/65	10/0	10/0	10/0	No	50/25%
COTS CPI and Critical Function SW	Vendor SwA	Vendor SwA	Vendor SwA	0	0	0	Yes	UNK
COTS (other than CPI and Critical Function) and NDI SW	No	No	No	0	0	0	No	UNK

Operational System						
	Failover Multiple Supplier Redundancy	**Fault Isolation**	**Least Privilege**	**System Element Isolation**	**Input checking / validation**	**SW load key**
Developmental CPI SW	30%	All	all	yes	All	All
Developmental Critical Function SW	50%	All	All	yes	All	all
Other Developmental SW	none	Partial	none	None	all	all
COTS (CPI and CF) and NDI SW	none	Partial	All	None	Wrappers/ all	all

Development Environment								
SW Product	**Source**	**Release testing**	**Generated code inspection p/a**					
C Compiler	No	Yes	50/20					
Runtime libraries	Yes	Yes	70/none					
Automated test system	No	Yes	50/none					
Configuration management system	No	Yes	NA					
Database	No	Yes	50/none					
Development Environment Access	Controlled access; Cleared personnel only							

Additional Guidance in PPP Outline and Guidance

Risk Assessment Methodology

Risk Assessment

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

Threat Analysis Results

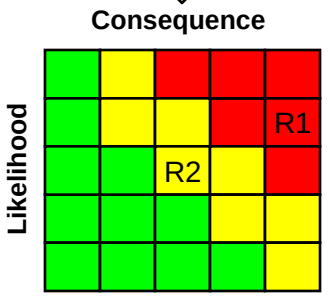
Supplier	Critical Components (HW, SW, Firmware)	TAC Findings
Supplier 1	Processor X	Potential Foreign Influence
	FPGA 123	Potential Foreign Influence
Supplier 2	SW Algorithm A	Cleared Personnel
	SW Module Y	Cleared Personnel

Risk Mitigation and Countermeasure Options

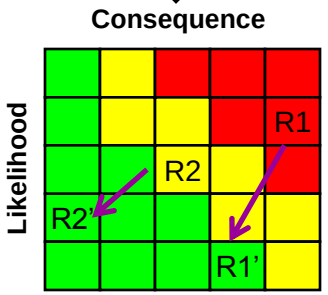
Consequence of Losing Mission Capability
Very High
High
Moderate
Low
Very Low

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

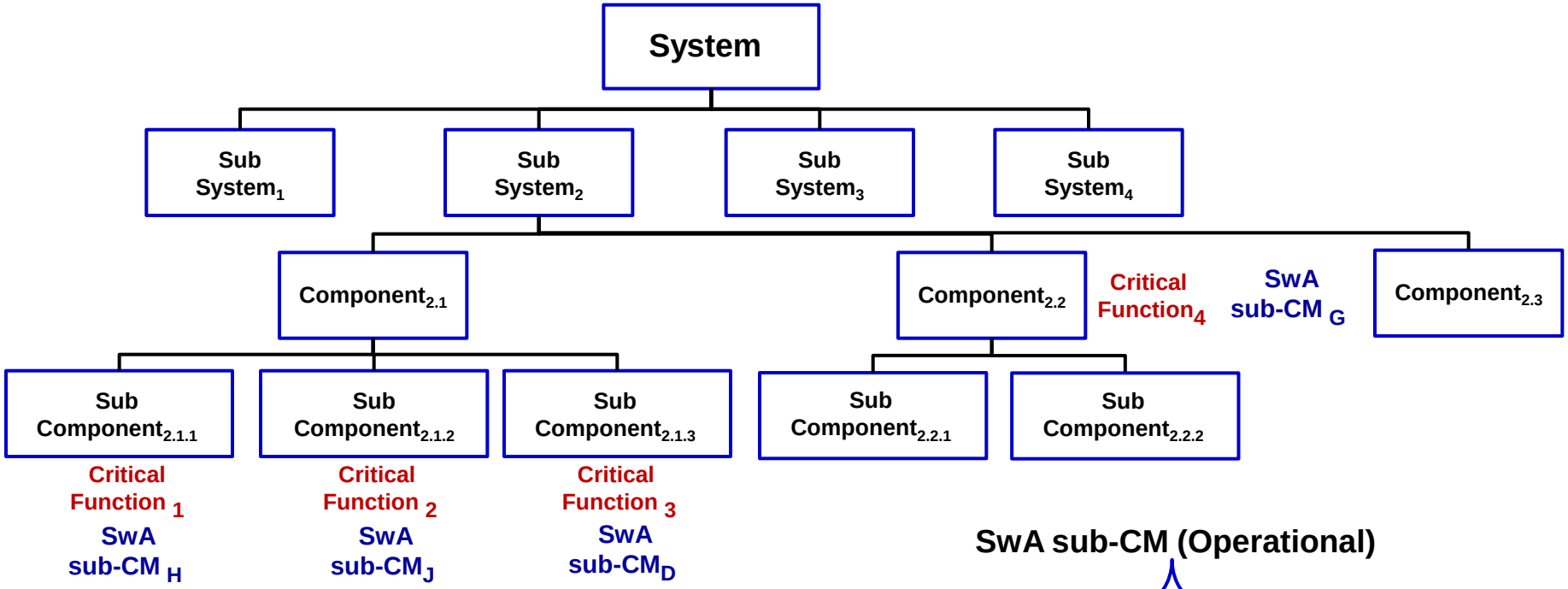
Initial Risk Posture



Risk Mitigation Decisions



Allocation of Countermeasures to Design: SwA Example



SwA sub-CM (Operational)

A. Application-layer Firewall
B. Virtualization
C. Sandboxing
D. Segregated SW functions
E. Intrusion Detection System
F. Honey pot System
G. SW Load Key
H. Authentication
I. SW Fault Tolerance
J. Least Privilege
K. Complete Mediation
L. Separation of Privilege
M. Safe memory allocation and management
N. Input Validation
O. Security aware error and exception handling
P. Non-informative error messages
Q. Cache purge

Wrap-Up

- **Program Protection needs industry support to succeed…**
  - How will you build the capability to implement?

- **Questions?**