Testing & Evaluation for Weapon System Security

March 3, 2009

Office of the Under Secretary of Defense
Acquisition, Technology and Logistics
Systems and Software Engineering Directorate

Agenda

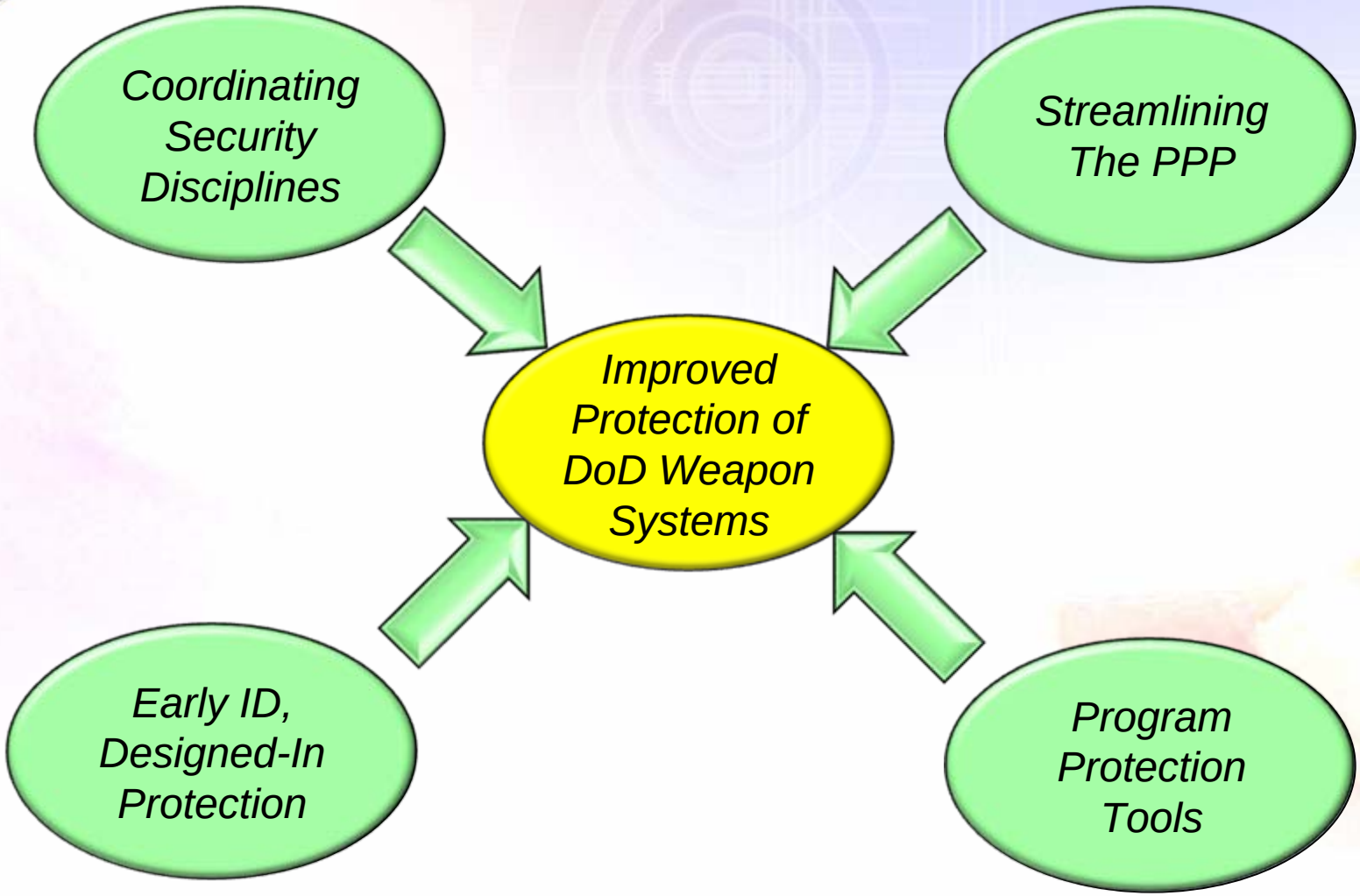
- **Today's Threats, Vulnerabilities**
- **Acquisition Security Policies**
- **Streamlining Acquisition Security**
  - Security Disciplines
  - Program Protection Plan
  - Designing-In Protection
- **Implementing Protection**
  - System Component Protection Best Practices & Tools
  - Evaluation of Protection
- **Summary**

Today's Threats & Vulnerabilities

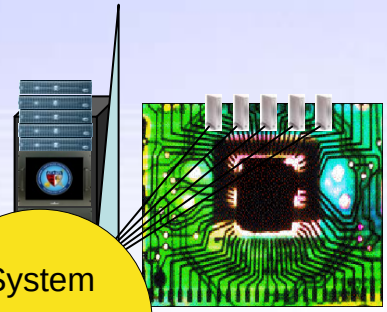
How are we verifying and validating that we are reducing the risk of these types of attacks in our systems?

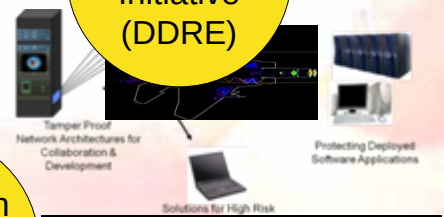
- **Threats: Nation-state, terrorist, criminal, rogue developer who:**
  - Gain control of IT/NSS/Weapons through supply chain opportunities
  - Exploit vulnerabilities remotely
- **Vulnerabilities: All IT/NSS/Weapons (incl. systems, networks, applications)**
  - Intentionally implanted logic (e.g., back doors, logic bombs, spyware)
  - Commercial software and circuit cards with embedded "phone home" functionality
- **Consequences: Stolen critical data & technology; corruption, denial of critical warfighting functionality**

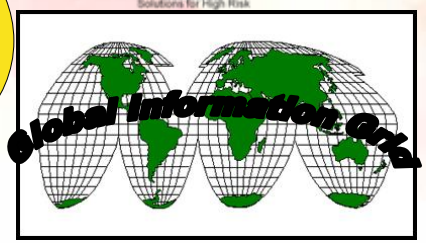
Improving DoD Program Protection



Numerous Security Disciplines







Program Protection (USD(I))

Trusted Micro-electronics (DTICS (DDRE, NII, IP))

Trusted Foundry (DDRE)

Center For Assured Software (NSA)

Quality Engineer

Configuration Manager

Reliability Engineer

Systems Engineer

Safety Engineer

Program Manager

Anti-Tamper (AF)

System Assurance (AT&L/NII)

Software Protection Initiative (DDRE)

Information Assurance (NII)

Protection implemented via multiple initiatives with multiple owners

Acquisition Security Policies

DODI 5200.39: integration point for policies, NOT replacement

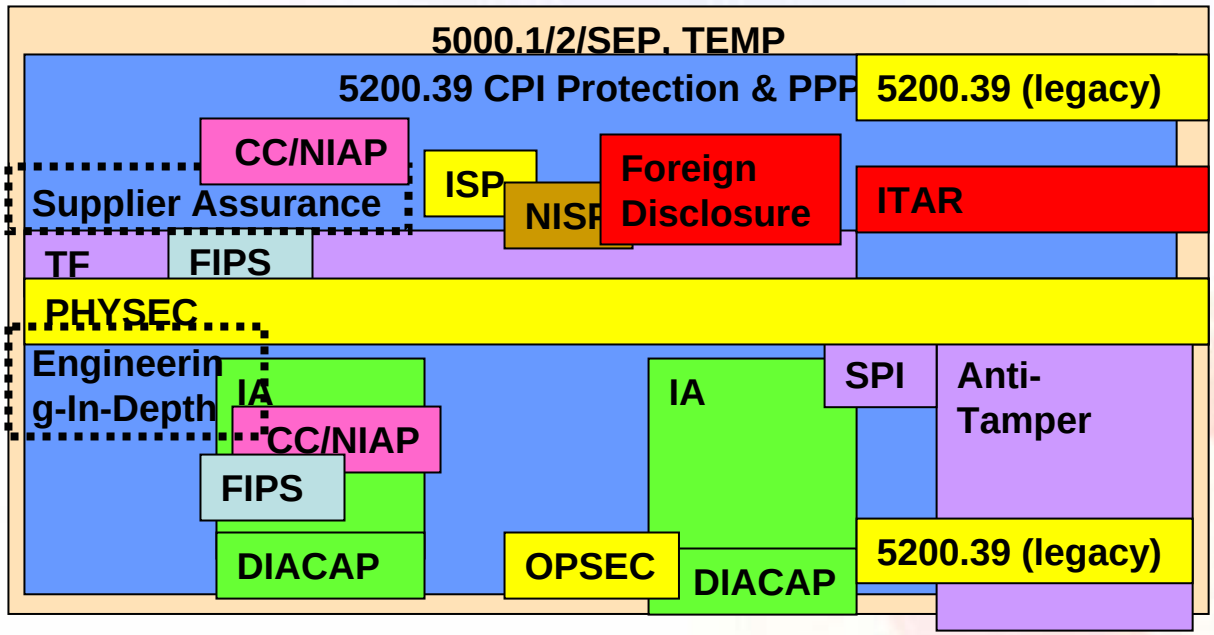
NEW CPI Protection Countermeasures

Defense-In-Depth

- Intelligence
- Supply Chain
- Engineering
- Certification
- Documented Plan

Component Protection Sought

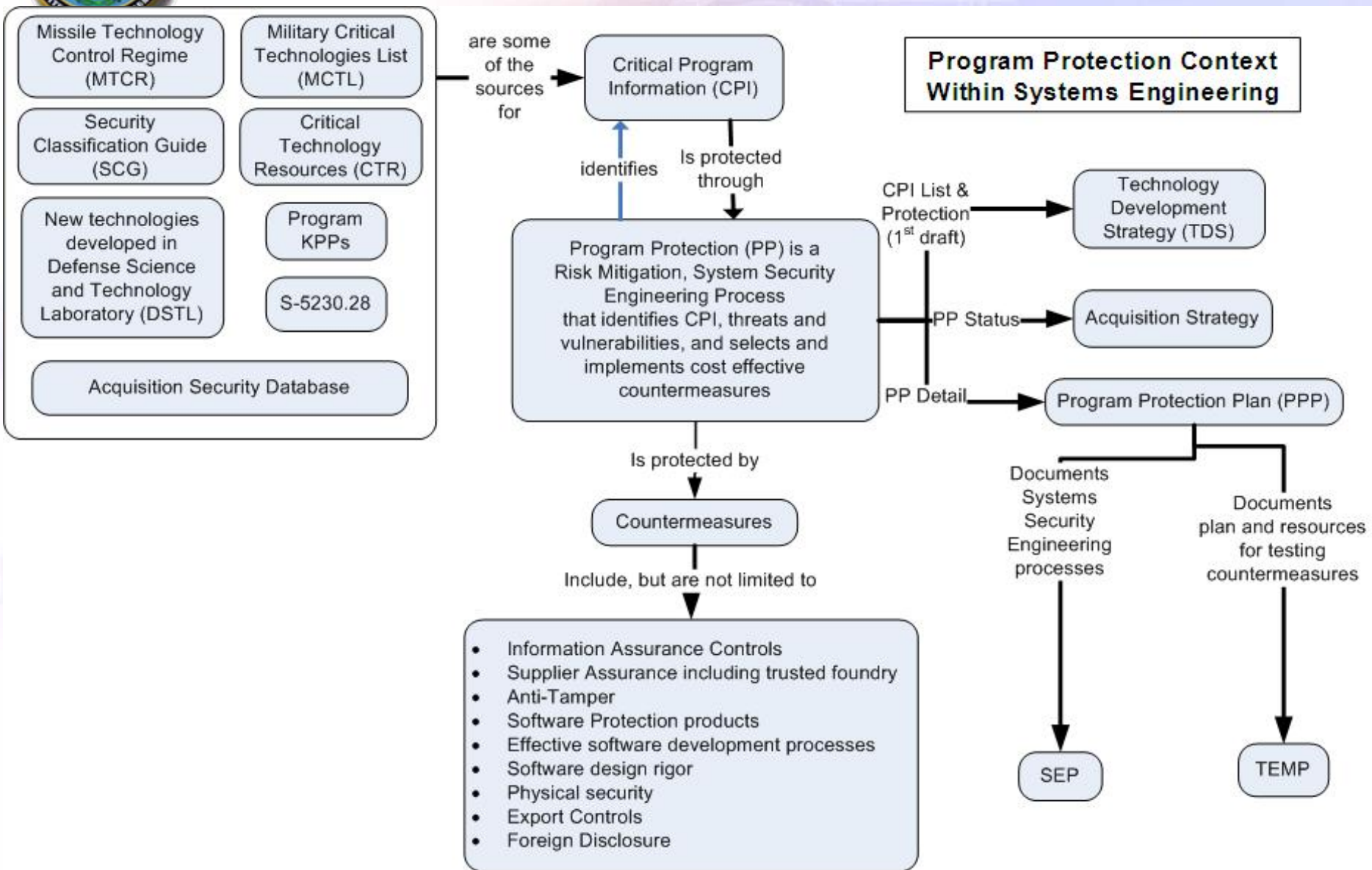
Critical Functionality		Critical Information		Critical Technology	
Custom	COTS	Classified	Un-Classified	Software	Hardware/ Firmware



Policy Ownership		
	USD(I)	
DoD – AT&L/S&T	DoD - CIO/DSS	DoD – AT&L
Dept. of State	DoD - CIO/DISA	NSA/CC
	DoD - USD(I)	NIST

DoD Controlled
Development/Operation

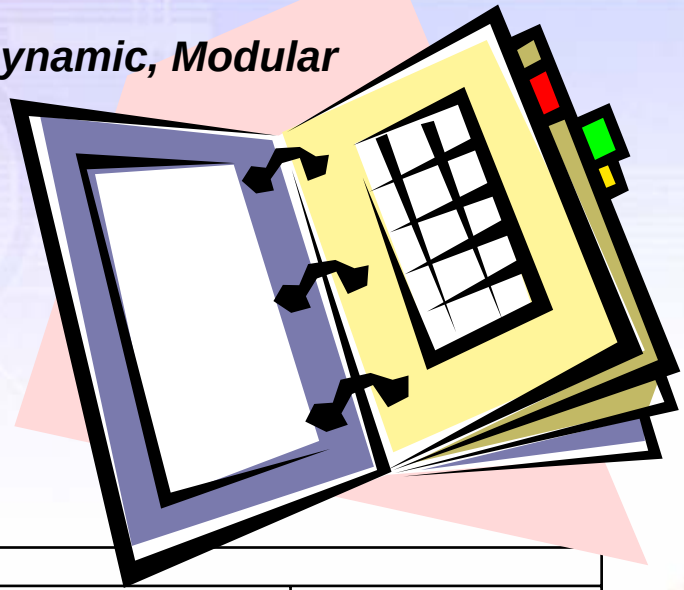
Systems Security Engineer Leads Integration of Security Resources



New PPP: Data Driven Format

Verbose, Static, Essay

Pithy, Dynamic, Modular



Critical Program Information (CPI)				
Critical Program Information	*Impact of Loss* *(Low, Med, Hi)*	*Reason (for each change in status)*	*List Locations* *(Lab(s), PMO, Contractor Name(s), Test Site(s))*	*Status Dates (watch, new, removed)*
GPS		New: Critical warfighting component	PMO, Contractor X	New 6/2006
Radar FPGA		New: target for hackers	PMO, Prime, Subcontractor Z	Watch 6/2007
Communication Card		Watch: US lead in technology Removed: No longer leading edge technology	N/A	New 4/1998 Removed 4/2007

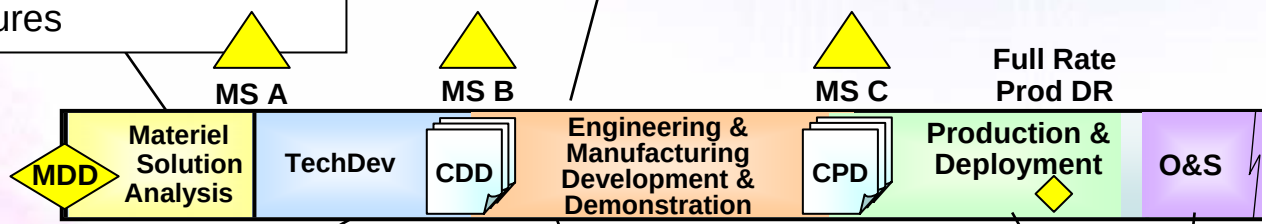
Example Format

Early, Designed-In Program Protection

• Acquisition Strategy, **TDS**, RFP, SEP, and TEMP must be revised to include PPP relevant information
• **Milestone Decision Authority approves PPP in addition to PM**

Streamlined Program Protection Plan
- **One-stop shopping for documentation of acquisition program security (ISP, IAS, AT appendices)**
- **Living document, easy to update, maintain**
- **Improve over time based on feedback**

• Identify draft CPI, estimated protection duration and S&T Lab countermeasures

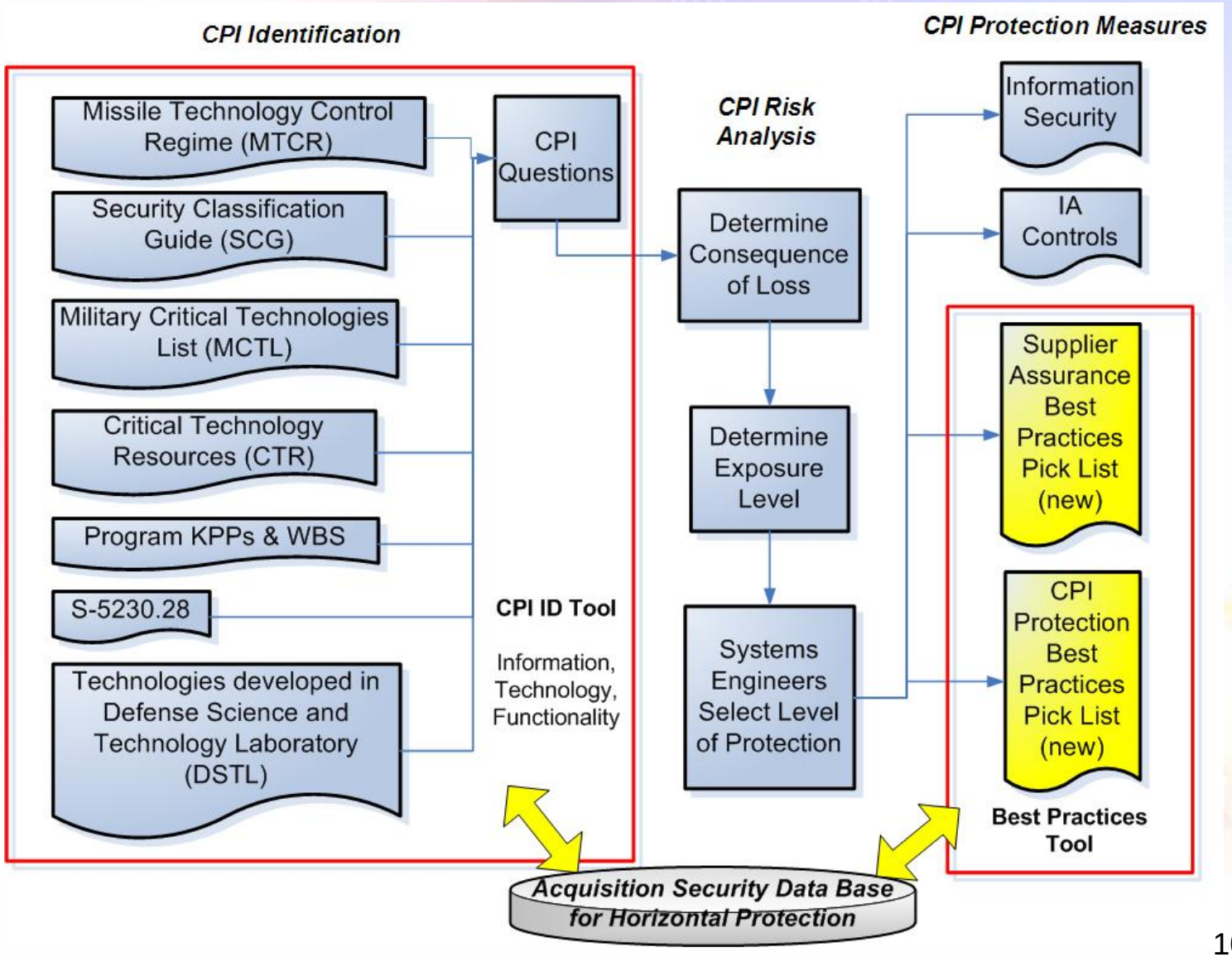


• Obtain threat assessments from Intel/CI, assess supplier risks
• Develop design strategy for CPI protection
• **Submit PPP to Acquisition Security Database (ASDB)**

• Contractor adds detail to Program Protection Plan
• Preliminary **verification and validation** that design meets assurance plans

• Enhance countermeasure information in Program Protection Plan (PPP)
• **Evaluate** that CPI Protection RFP requirements have been met

Program Protection Tools



Best Practice Format

DRAFT

- **Title:** Name of best practice
- **Requirement:** Sample requirement language for inclusion in RFP
- **Application:** Explanation of conditions under which best practice should be applied
- **Evaluation:** Recommended technique for evaluation for each life cycle phase
- **Metrics:** Criteria for successful implementation
- **Cost:** Rough estimate of cost (order of magnitude)
- **References:** sources of information and SMEs that contributed to development of this control
- **Background:** supporting anecdotes/evidence

Best Practice Example

Not Validated For Use – For Example Only

- **Title:** Code Static Analysis
- **Requirement:** Implement static code analysis tool for use during software development.
- **Application:** automated method of detecting and eliminating bugs early in the development cycle
- **Evaluation:** Analysis of code improvements and remaining types of weaknesses
- **Metric(s):** types of software problems eliminated
- **Cost:** $250/user
- **References:** samate.nist.gov, DoD Labs
- **Background:** DoD labs and commercial vendors have static code analysis tools

CPI Protection Evaluation

What should the CPI Verification and Validation Strategy be?

Forms of Evaluation:

- **Analysis**
  - Pre-MS B analyze planned countermeasures for sufficiency versus threats and vulnerabilities
- **Testing**
  - System Security Certification?
  - OT&E attack scenarios?
  - DT&E insider attack scenarios?
  - Security vulnerability testing?
  - Automated identification and removal of malicious code?
- **Monitoring**
  - Survey public domain information
  - Detect, record, act and report CPI loss, AT breaches

Summary

- **Program Protection strategy provides**
  - Overarching framework and process to integrate acquisition security policies and resources early in the life cycle
  - One-stop shopping for acquisition security documentation
  - Best practice tools to support implementation
- **Current Test and Evaluation resources are still fragmented across IA, Anti-Tamper, Software, etc. a comprehensive, integrated strategy for T&E of program protection is under development**

We welcome feedback on PP Streamlining and T&E

www.acq.osd.mil/sse/

Christine.hines.ctr@osd.mil

(703) 682-5309

QUESTIONS?

Streamlining Program Protection