System Security Engineering and Program Protection Integration into SE

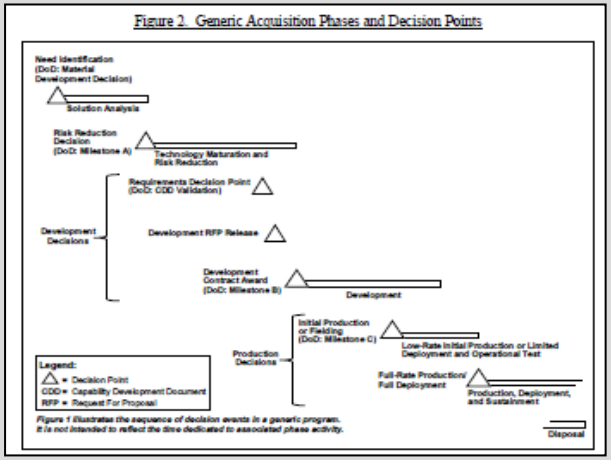
Melinda Reed
Deputy Director for Program Protection
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

17th Annual NDIA Systems Engineering Conference
Springfield, VA | October 29, 2014

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, and/or degrade system behavior
- ***Vulnerabilities:***
  - All systems, networks, and applications
  - Intentionally implanted logic
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- ***Consequences:***
  - Loss of critical data and technology
  - System corruption
  - Loss of confidence in critical warfighting capability; mission impact

Access points are throughout the lifecycle…



…and across multiple supply chain entry points

- Government
- Prime, subcontractors
- Vendors, commercial parts manufacturers
- 3rd party test/certification activities

Many Program Protection Risks to Consider

Quality Escape

Product defect/inadequacy introduced either through mistake or negligence during design, production, and post-production handling resulting in the introduction of deficiencies, vulnerabilities, and degraded life-cycle performance

Reliability Failure

Mission failure in the field due to environmental factors unique to military and aerospace environment factors such as particle strikes, device aging, hot-spots, electro-magnetic pulse, etc.

Fraudulent Product

Counterfeit and other than genuine and new devices from the legally authorized source including relabeled, recycled, cloned, defective, out-of-spec, etc.

Malicious Insertion

The intentional insertion of malicious hard/soft coding, or defect to enable physical attacks or cause mission failure; includes logic bombs, Trojan 'kill switches' and backdoors for unauthorized control and access to logic and data

Anti-Tamper

Unauthorized extraction of sensitive intellectual property using reverse engineering, side channel scanning, runtime security analysis, embedded system security weakness, etc.

Emerging Threats

New threats, cyber security attacks, and trust issues that combine two or more threats

DoD Program Protection focuses on risks posed by adversary actors

Program Protection in Context

- **Program Protection:** The integrating process for managing risks to advanced technology and mission-critical system functionality from foreign collection, design vulnerability or supply chain exploit/insertion, and battlefield loss throughout the acquisition lifecycle.
  PPP Outline and Guidance

- **Systems 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.
  DoDI 5200.44

- **Critical Program Information (CPI):** Elements or components of a research, development, and acquisition (RDA) program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability.
  DoDI 5200.39

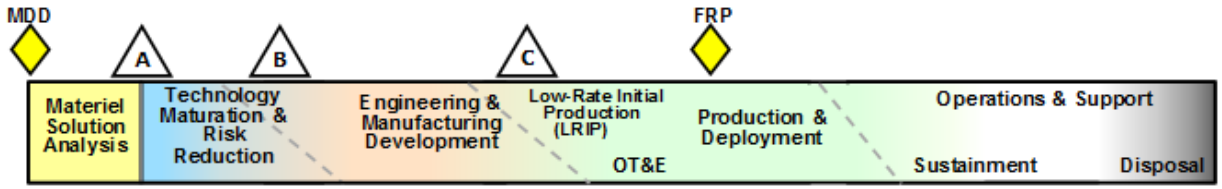
For more information:
http://www.acq.osd.mil/se/pg/policy.html#sa
http://www.acq.osd.mil/se/pg/guidance.html#sa

Program Protection Interim DoDI 5000.02

- **Program Protection is the integrating process for managing risks to DoD warfighting capability from foreign intelligence collection; from hardware, software, and cyber vulnerability or supply chain exploitation; and from battlefield loss throughout the system life cycle.**
  - Also supports international partnership building and cooperative opportunities objectives by enabling the export of capabilities without compromising underlying U.S. technology advantages

- **Program managers will employ system security engineering practices and prepare a PPP to guide their efforts and the actions of others to manage the risks to critical program information and mission-critical functions and components associated with the program**
  - The PPP will be submitted for MDA approval at each Milestone review, beginning with Milestone A

- **Program managers will describe in their PPP:**
  - Critical Program Information, mission-critical functions, and critical components
  - Threats to and vulnerabilities of these items
  - Plans to apply countermeasures to mitigate associated risks
  - Plans for exportability and potential foreign involvement
  - The Cybersecurity Strategy and Anti-Tamper plan are included as appendices



What Are We Protecting?

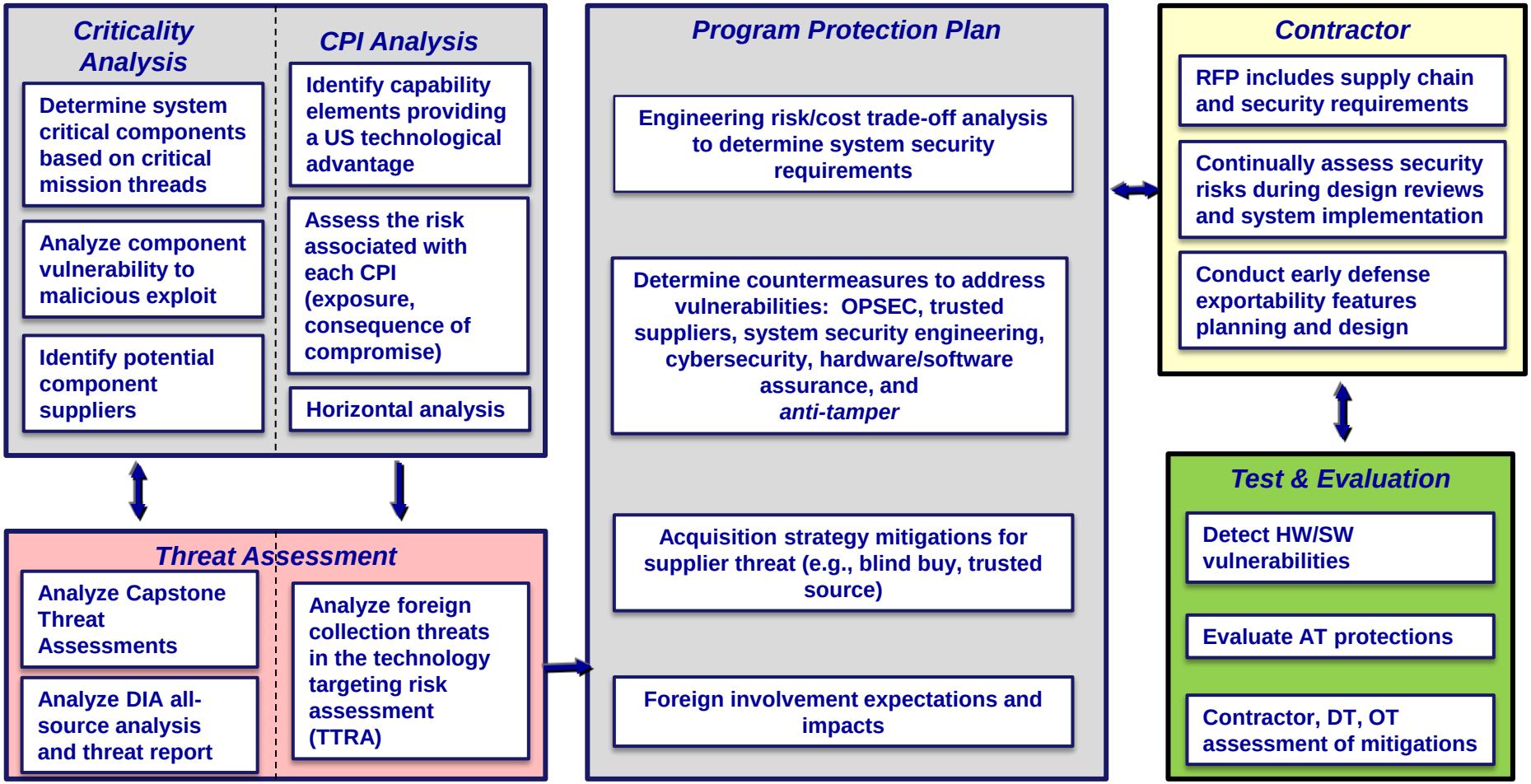
Program Protection Planning

Interim DoDI 5000.02

DoDI 5200.39 Change 1, dated Dec 2010	DoDI 5200.44	DoDI 8500 Series DoDI 8500.01E DoDI 8582.01
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

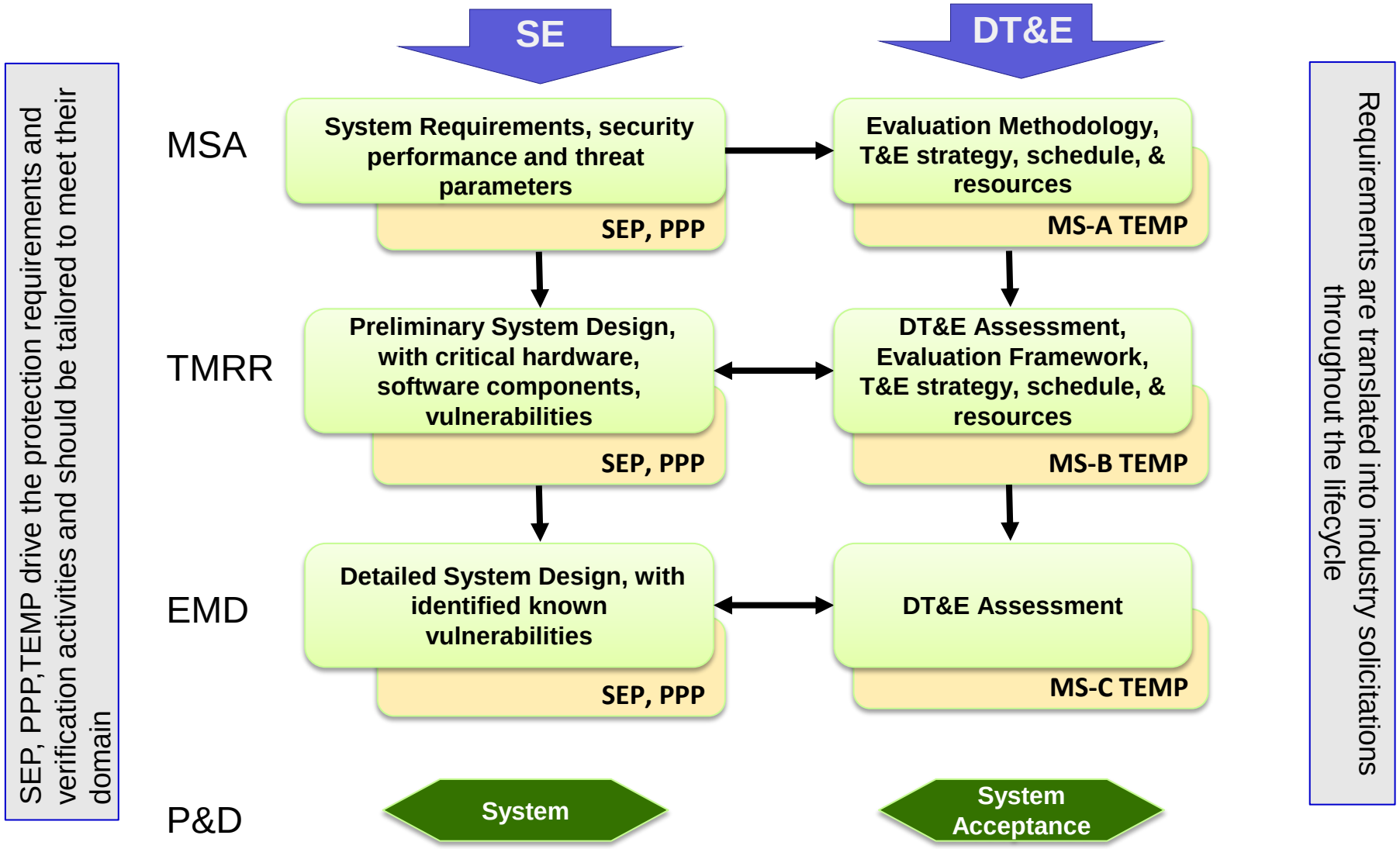
Protecting Warfighting Capability Throughout the Lifecycle

PPP Methodology



Program Protection Activity - Integral Part of SE Process

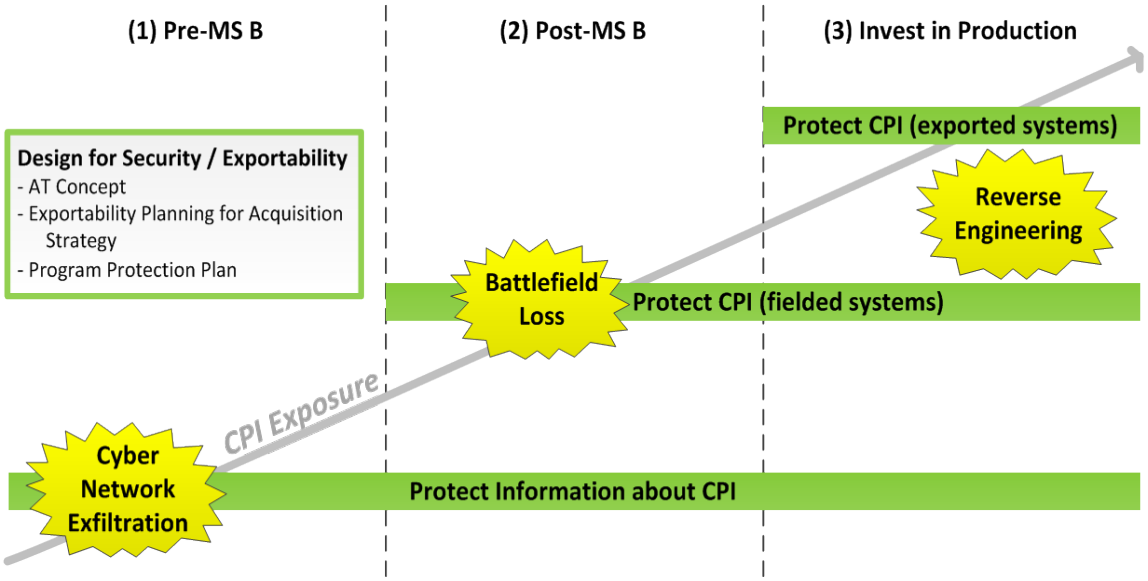
SE, SSE and DT&E are Mutually Supportive



CPI Protection Throughout the Life Cycle

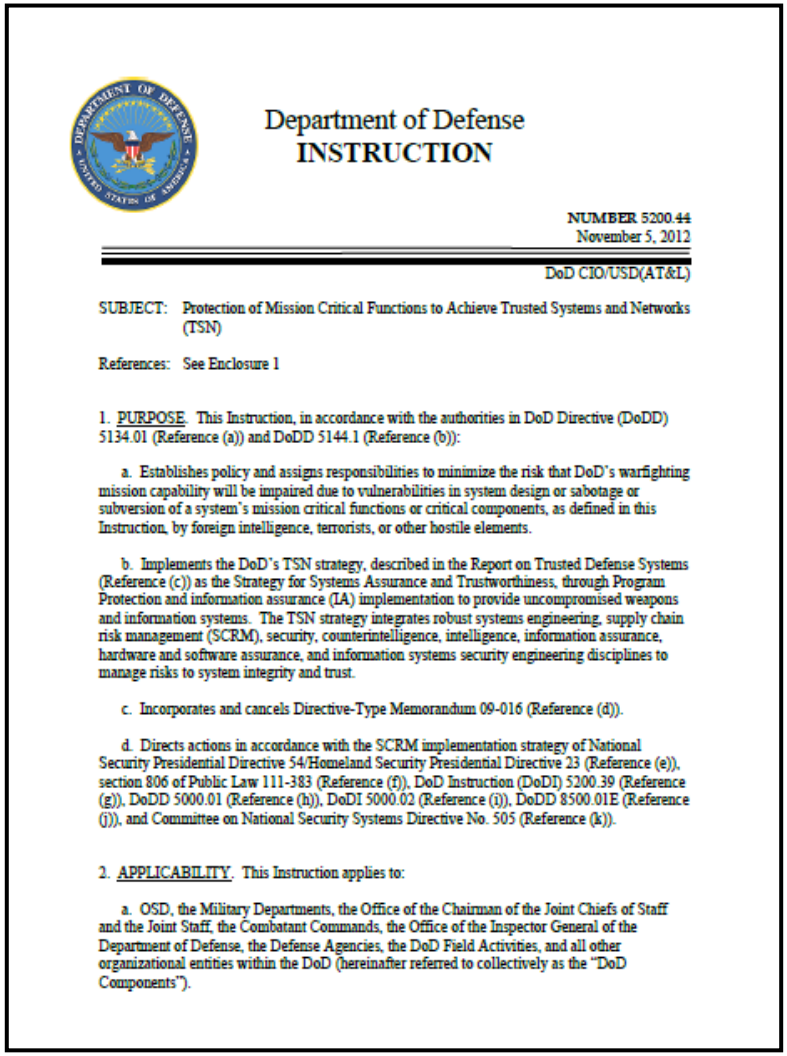
- **Anti-Tamper (AT) is the set of system engineering activities (hardware and/or software techniques) designed into the system architecture to protect CPI against:**
  - Unwanted technology transfer (e.g. technology loss)
  - Potential adversary countermeasure development
  - System modification to enhance capability/performance

- **Anti-Tamper guidance**
  - An AT Concept prepared at Milestone (MS) A
  - An AT Plan is required at MS B
  - Submitted as an annex to the program's PPP



Balance CPI exposure — threat — consequence of loss

Protecting Components
DoDI 5200.44



Department of Defense
INSTRUCTION

NUMBER 5200.44
November 5, 2012

DoD CIO/USD(AT&L)

SUBJECT: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

References: See Enclosure 1

1. PURPOSE. This Instruction, in accordance with the authorities in DoD Directive (DoDD) 5134.01 (Reference (a)) and DoDD 5144.1 (Reference (b)):

a. Establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components, as defined in this Instruction, by foreign intelligence, terrorists, or other hostile elements.

b. Implements the DoD's TSN strategy, described in the Report on Trusted Defense Systems (Reference (c)) as the Strategy for Systems Assurance and Trustworthiness, through Program Protection and information assurance (IA) implementation to provide uncompromised weapons and information systems. The TSN strategy integrates robust systems engineering, supply chain risk management (SCRM), security, counterintelligence, intelligence, information assurance, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust.

c. Incorporates and cancels Directive-Type Memorandum 09-016 (Reference (d)).

d. Directs actions in accordance with the SCRM implementation strategy of National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (e)), section 806 of Public Law 111-383 (Reference (f)), DoD Instruction (DoDI) 5200.39 (Reference (g)), DoDD 5000.01 (Reference (h)), DoDI 5000.02 (Reference (i)), DoDD 8500.01E (Reference (j)), and Committee on National Security Systems Directive No. 505 (Reference (k)).

2. APPLICABILITY. This Instruction applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

- **Implements the DoD's Trusted Systems and Networks (TSN) strategy**
- **Manage risk of mission-critical function and component compromise throughout lifecycle of key systems by utilizing**
  - Criticality Analysis as the systems engineering process for risk identification
  - Countermeasures: Supply chain risk management, software assurance, secure design patterns
  - Intelligence analysis to inform program management
- **Codify trusted supplier requirement for DoD-unique application-specific integrated circuits (ASICs)**
- **Document planning and accomplishments in program protection and information assurance activities**

Protecting Information

"America must also face the rapidly growing threat from cyber-attacks… We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy.

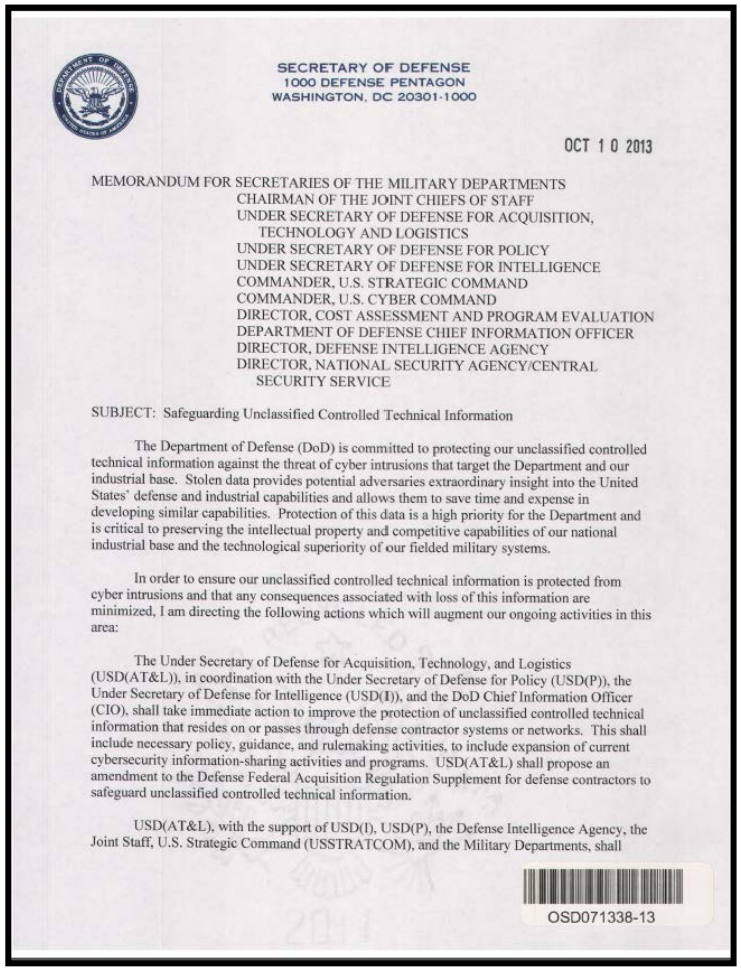
"We are going to aggressively protect our intellectual property. Our single greatest asset is the innovation and the ingenuity and creativity of the American people. It is essential to our prosperity and it will only become more so in this century."

President Barack Obama
February 2013

DoD efforts to advance cyber security in the Defense Industrial Base (DIB) include:

- DIB Cyber Security/Information Assurance (CS/IA) Program, and its optional enhanced component the DIB Enhanced Cybersecurity Services (http://dibnet.dod.mil)
- Standards development in collaboration with Industry
- Reinforcing protection of technical information in contract requirements

Safeguarding Unclassified Controlled Technical Information



SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

OCT 10 2013

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY AND LOGISTICS
UNDER SECRETARY OF DEFENSE FOR POLICY
UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
COMMANDER, U.S. STRATEGIC COMMAND
COMMANDER, U.S. CYBER COMMAND
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
DIRECTOR, DEFENSE INTELLIGENCE AGENCY
DIRECTOR, NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

SUBJECT: Safeguarding Unclassified Controlled Technical Information

The Department of Defense (DoD) is committed to protecting our unclassified controlled technical information against the threat of cyber intrusions that target the Department and our industrial base. Stolen data provides potential adversaries extraordinary insight into the United States' defense and industrial capabilities and allows them to save time and expense in developing similar capabilities. Protection of this data is a high priority for the Department and is critical to preserving the intellectual property and competitive capabilities of our national industrial base and the technological superiority of our fielded military systems.

In order to ensure our unclassified controlled technical information is protected from cyber intrusions and that any consequences associated with loss of this information are minimized, I am directing the following actions which will augment our ongoing activities in this area:

The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), in coordination with the Under Secretary of Defense for Policy (USD(P)), the Under Secretary of Defense for Intelligence (USD(I)), and the DoD Chief Information Officer (CIO), shall take immediate action to improve the protection of unclassified controlled technical information that resides on or passes through defense contractor systems or networks. This shall include necessary policy, guidance, and rulemaking activities, to include expansion of current cybersecurity information-sharing activities and programs. USD(AT&L) shall propose an amendment to the Defense Federal Acquisition Regulation Supplement for defense contractors to safeguard unclassified controlled technical information.

USD(AT&L), with the support of USD(I), USD(P), the Defense Intelligence Agency, the Joint Staff, U.S. Strategic Command (USSTRATCOM), and the Military Departments, shall

OSD071338-13

- **Secretary of Defense Memorandum, October 10, 2013**
  - Emphasizes DoD commitment to preserving the intellectual property (IP) and competitive capabilities of the Defense Industrial Base (DIB) and the technological superiority of our fielded military systems.
- **Key Goals**
  - Protect DoD unclassified controlled technical information from cyber intrusions
  - Minimize the consequences associated with loss of this information
- **Augments current activities**
  - Re-emphasizes the DIB Cyber Security/ Information Assurance (CS/IA) Program

DFARS Clause 252.204-7012: Safeguarding Unclassified Controlled Technical Information*

- **Published November 18, 2013**
  - Clause affects all new contracts that contain, or will contain unclassified controlled technical information
  - Includes flow down to all subcontracts
- **Purpose: Establish minimum requirements for DoD unclassified controlled technical information on contractor information systems**
  - Requires contractors implement minimum set of information security controls
    - 51 information security controls from NIST SP 800-53, Revision 4
    - Combination of Technical, Process, Awareness, and Training measures
  - Requires contractors report cyber incident and compromises
  - Requires contractor actions to support DoD damage assessment as needed
- **Incident Reporting**
  - Reporting includes:
    - DoD contracts and subcontractor information affected by a cyber incident or compromise
    - DoD programs, platforms, or systems involved
    - Description of DoD technical information compromised
  - Reported information does not include signatures or other threat actor indicators

*http://www.acq.osd.mil/dpap/dars/dfars/html/current/204_73.htm

Major Actions Underway

- **Updating Program Protection guidance and training**
  - Establishing a discipline for system security engineering
- **Implementing DFARS Clause 252.204-7012, "Safeguarding Unclassified Controlled Technical Information"**
  - Working with industry and contracting community
  - Providing guidance, working through procedures
- **Joint Federated Assurance Center for HW/SW**
  - Required by Section 937 of FY14 NDAA
  - Provides network of vulnerability analysis detection and mitigation support to programs; and R&D improvement (resource limited)
- **Trusted microelectronics strategy to move beyond ASICs**
  - FPGAs, Microprocessors, Logic Application Specific Standard Products, Memories, A-D Converters, Interface Chips
- **Anti-Tamper Policy and Guidance updates**
  - DoD Instruction for AT, AT Technology oversight, guidance updates

Our Focus on SSE and SE

- **DoD is putting policy in place for a risk-based cost benefit trade-off process to protect systems, their supply chain, and their software development**
- **DoD is emphasizing the importance of SSE within systems engineering and its contribution to the design of systems by:**
  - Ensuring that program protection is addressed during the SE technical reviews
  - Incorporating program protection and system security engineering requirements and processes into engineering development contracts
  - Working with industry and standards groups revitalize system security engineering
- **Industry is playing an important role in the DoD SSE initiative by:**
  - Investing in research and processes to protect systems, the supply chain and the software development
  - Developing their SE and SSE processes and skills

DoD efforts are targeting integration of system security engineering considerations throughout the system life cycle

Systems Engineering: Critical to Defense Acquisition










Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

For Additional Information

Melinda Reed

ODASD, Systems Engineering

571-372-6562 | Melinda.K.Reed4.civ@mail.mil

Paul Popick

ODASD, Systems Engineering

571-372-6467 | Paul.R.Popick.ctr@mail.mil

JeanPaul LeSaint

ODASD, Systems Engineering

571-372-6554 | JeanPaul.R.LeSaint.ctr@mail.mil

Additional References

DFARS Clause 252.204-7012: Minimum Security Controls for Safeguarding

Access Control (AC)
- AC-2: Account Management
- AC-3(4): Access Enforcement
- AC-4: Information Flow Enforcement
- AC-6: Least Privilege
- AC-7: Unsuccessful Logon Attempts
- AC-11(1): Session Lock
- AC-17(2): Remote Access
- AC-18(1): Wireless Access
- AC-19: Access Control for Mobile Devices
- AC-20(1): Use of External Information Systems
- AC-20(2): Use of External Information Systems
- AC-22: Publicly Accessible Content

Awareness and Training (AT)
- AT-2: Security Awareness Training

Audit and Accountability (AU)
- AU-2: Audit Events
- AU-3: Content of Audit Records
- AU-6(1): Audit Review, Analysis and Reporting
- AU-7: Audit Reduction and Report Generation
- AU-8: Timestamps
- AU-9: Protection of Audit Information

Configuration Management (CM)
- CM-2: Baseline Configuration
- CM-6: Configuration Settings
- CM-7: Least Functionality
- CM-8: Information System Component Inventory

Contingency Planning Acquisition (CP)
- CP-9: Information System Backup

Identification and Authentication
- IA-2: Identification and Authentication (Organizational Users)
- IA-4: Identifier Management
- IA-5(1): Authenticator Management

Incident Response Integrity (IR)
- IR-2: Incident Response Training
- IR-4: Incident Handling
- IR-5: Incident Monitoring
- IR-6: Incident Reporting

Maintenance (MA)
- MA-4(6): Non-local Maintenance
- MA-5: Maintenance Personnel
- MA-6: Timely Maintenance

Media Protection (MP)
- MP-4: Media Storage
- MP-6: Media Sanitization

Physical & Environmental (PE)
- PE-2: Physical Access Authorizations
- PE-3: Physical Access Control
- PE-5: Access Control for Output Devices

Program Management (PM)
- PM-10: Security Authorization Process

Risk Assessment (RA)
- RA-5: Vulnerability Scanning

System and Communication Protection (SC)
- SC-2: Application Partitioning
- SC-4: Information in Shared Resources
- SC-7: Boundary Protection
- SC-8(1): Transmission Confidentiality
- SC-13: Cryptographic Protection
- SC-15: Collaborative Computing Devices
- SC-28: Protection of Information at Rest

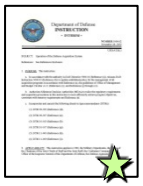
System & Information (SI)
- SI-2: Flaw Remediation
- SI-3: Malicious Code Protection
- SI-4: Information System Monitoring

NIST SP 800-53 (Rev 4), "Security and Privacy Controls for Federal Information Systems and Organizations"
- Comprehensive set of security privacy controls addressing Federal security requirements
- Development included participation from Civil, Defense, and Intelligence communities
- Controls are tailorable to an organization's processes

DoDI 5230.24
Technical Information Definition

- **The term includes technical data or computer software of any kind that can be used, or adapted for use, in the design, production, manufacture, assembly, repair, overhaul, processing, engineering, development, operation, maintenance, adapting, testing, or reconstruction of goods or materiel; or any technology that advances the state of the art, or establishes a new art, in an area of significant military applicability in the United States.**
  - The data may be in tangible form, such as a blueprint, photograph, plan, instruction, or an operating manual, or may be intangible, such as a technical service or oral, auditory, or visual descriptions.
  - Examples of technical data include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software.

Program Protection Integrated in Policy



Interim DoDI 5000.02 Operation of the Defense Acquisition System

- Regulatory requirement for Program Protection Plan at Milestones A, B, C and FRP/FDD

DoDI 5200.39 Critical Program Information (CPI) Protection Within the DoD

- Assigns responsibility for Counterintelligence, Security, and System Engineering support for the identification and protection of CPI

DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks

- Establishes policy and responsibilities to minimize the risk that warfighting capability will be impaired due to vulnerabilities in system design or subversion of mission critical functions or components (including software, microelectronics)

DoDI 4140.67 DoD Counterfeit Prevention Policy

- Establishes policy and assigns responsibility to prevent the introduction of counterfeit material at any level of the DoD supply chain

DoDI 8500.01 Cybersecurity

- Establishes a DoD cybersecurity program to protect and defend DoD information and information technology

- Update in process

RFP Sections

RFP Package

- Section A: Solicitation Contract Form
- Section B: Supplies or services and prices/costs
- **Section C: Description/specifications/work statement**
  - **System Requirements Document (SRD - SPEC)**
  - **Statement of Work (SOW)**
  - **Contract Deliverable Requirements List (CDRLs)**
- Section D: Packaging and marking
- Section E: Inspection and Acceptance
- Section F: Deliveries or performance
- Section G: Contract administration data
- Section H: Special contract requirements
- **Section I: Contract Clauses**
- Section J: List of Documents, Exhibits, and other Attachments
- Section K: Representations, Certification, and Other Statements of Offerors
- **Section L: Instructions, conditions, and notices to offerors**
- **Section M: Evaluation factors for award**

- **Incorporate Protection Requirements and Designs**
  System Requirements Document (SRD), Specification, or equivalent
- **Incorporate Protection Activities to develop protection requirements, designs and to evaluate those protections**
  Statement of Work (SOW), Statement of Objectives (SOO), Performance Work Statement (PWS), or equivalent
- **Contract Deliverable Requirements List (CDRLs)**
  Contract Data Item with Data Item Description (DID)

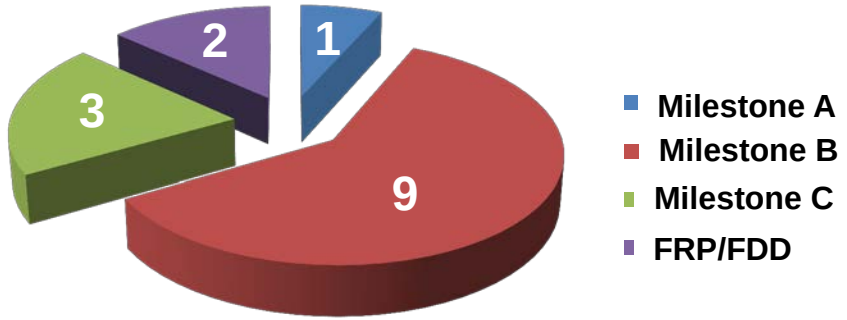
- **Defense Federal Acquisition Regulation (DFAR)**

- **As part of the evaluation request a contractor description of their system security protections and the protection activities to be performed during the acquisition.**
- Sections L and M

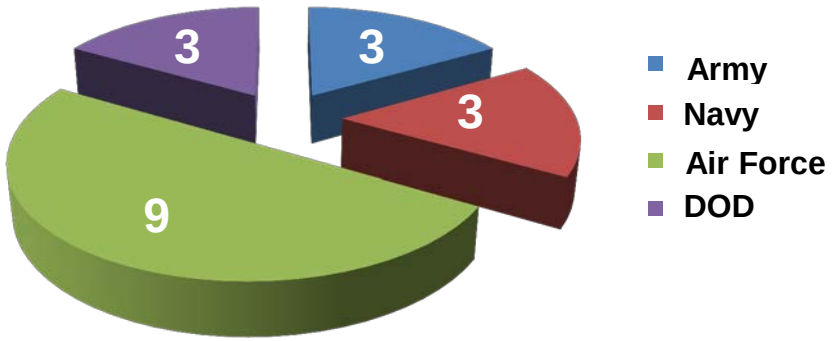
PPP Approval Statistics Since Outline and Guidance Signed

52 PPPs Approved	
FY 2010	4
FY 2011	7
FY 2012	5
FY 2013	18
FY 2014	18

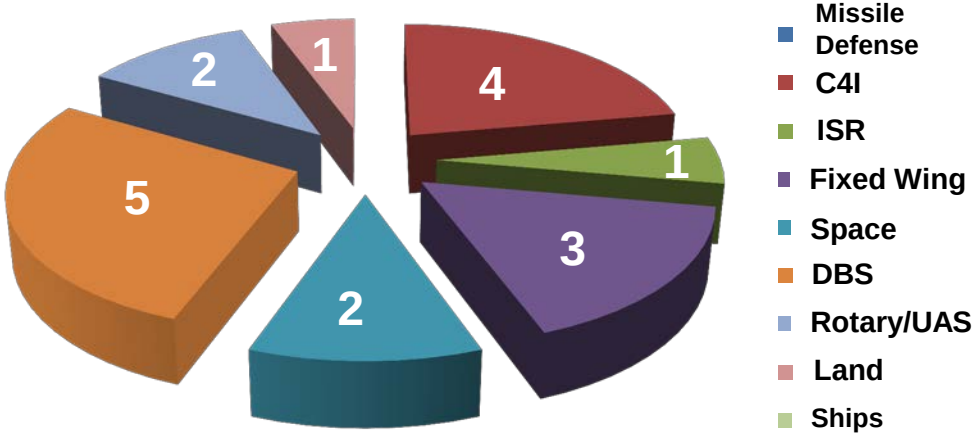
FY14 PPPs by Milestone



FY14 PPPs by Service



FY14 PPPs by Domain



Program Protection Outline and Guidance signed 18 July 2011