



# Comprehensive Program Protection and Trusted Microelectronics

**Kristen Baldwin**

**Principal Deputy**

**Office of the Deputy Assistant Secretary of Defense  
for Systems Engineering (DASD(SE)), OUSD(AT&L)**

**NDIA Trusted Microelectronics Workshop  
June 28, 2013**



# Why the Focus on Trusted 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
  - Lack of SCRM
  - Intentionally implanted logic
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- **Traditional Consequences: Loss of critical data, technology or capability**
- **Emerging Consequences: Loss of manufacturing technology, intellectual property and 'know how'**
- **All can result in loss of critical warfighting capability**

*Today's acquisition environment paradigm change has introduced new vulnerabilities:*

Stand-alone systems	>>>	Networked systems
Some software functions	>>>	Software-intensive
Known supply base	>>>	Prime Integrator, hundreds of suppliers
CPI (technologies)	>>>	CPI and critical components



# DASD, Systems Engineering



**DASD, Systems Engineering**  
**Stephen Welby**  
**Principal Deputy Kristen Baldwin**

**Systems Analysis**  
 Kristen Baldwin (Acting)

*Addressing Emerging Challenges on the Frontiers of Systems Engineering*

Analysis of Complex Systems/Systems of Systems  
 Program Protection/Acquisition Cyber Security  
 University, FFRDC and Industry Engineering and Research  
 Modeling and Simulation

**Major Program Support**  
 James Thompson

*Supporting USD(AT&L) Decisions with Independent Engineering Expertise*

Engineering Assessment / Mentoring of Major Defense Programs  
 Program Support Reviews  
 OIPT / DAB / ITAB Support  
 Systems Engineering Plans  
 Systemic Root Cause Analysis

**Mission Assurance**  
 Nicholas Torelli

*Leading Systems Engineering Practice in DoD and Industry*

Systems Engineering Policy & Guidance  
 Development Planning/Early SE  
 Specialty Engineering (System Safety, Reliability and Maintainability Engineering, Quality, Manufacturing, Producibility, Human Systems Integration)  
 Counterfeit Prevention  
 Technical Workforce Development  
 Standardization

**Providing technical support and systems engineering leadership and oversight to USD(AT&L) in support of planned and ongoing acquisition programs**



# 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 trusted and critical components
  - Provide PMs with criticality 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 automated vulnerability detection tools and capabilities for software
  - Technology investment to advance secure software, hardware, and system design methods





# What Are We Protecting?

## Program Protection Planning

DoDI 5000.02

DoDI 5200.39

DoDI 5200.44

DoDI 8500 Series  
DoDI 8582.01

### Technology

**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

### Components

**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

### Information

**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

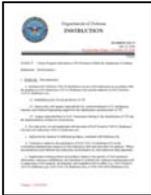
**Countermeasures:** Information Assurance, Classification, Export Controls, Security, etc.

**Focus:** "Keep critical information from getting out" by protecting data

**Protecting Warfighting Capability Throughout the Life Cycle**



# Program Protection Integrated in Policy



## DoDI 5000.02 Operation of the Defense Acquisition System

- Regulatory Requirement for Program Protection Plan at Milestones A, B, C and FRP/FDD
- References DoDI 5200.39



## DoDI 5200.39 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



## 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



## DoDI 8500.01E Information Assurance

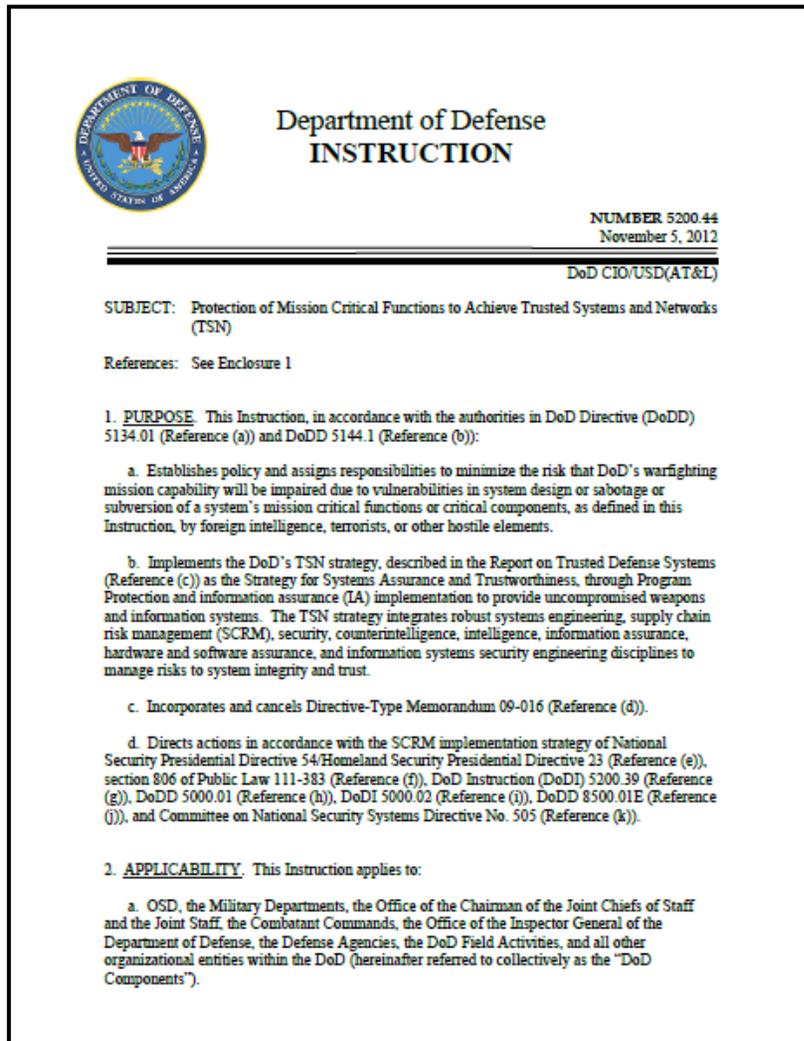
- Establishes policy and assigns responsibilities to achieve DoD information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare

DoD Issuances Website: <http://www.dtic.mil/whs/directives/corres/ins1.html>



# DoDI 5200.44

## Trusted Systems and Networks



- Implements the DoD's Trusted Systems and Networks (TSN) strategy
- Manage risk of mission-critical function and potential component compromise throughout the lifecycle of key systems by utilizing
  - Criticality Analysis as the systems engineering process for component risk identification
  - Application of Countermeasures: Supply chain risk management, software assurance, secure design patterns
  - Intelligence analysis to inform program management of potential counterfeits
- Codify trusted supplier requirements for DoD-unique application-specific integrated circuits (ASICs)
  - Establish a baseline of trust for ASIC components used in critical systems



# Program Protection Guidance



## **Program Protection Plan Outline & Guidance, dated 18 Jul 2011**

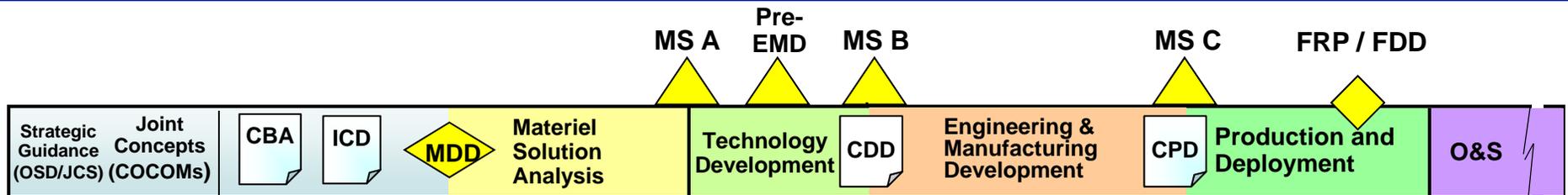
- **Focal point for documenting Program security activities, including:**
  - Plans for identifying and managing risk to CPI and critical functions and components
  - Responsibilities for execution of comprehensive program protection
  - Tables of actionable data, not paragraphs of boilerplate
  - End-to-end system analysis and risk management
- **<http://www.acq.osd.mil/se/docs/PPP-Outline-and-Guidance-v1-July2011.pdf>**

## **Defense Acquisition Guidebook Chapter 13, “Program Protection”**

- **Provides implementation guidance for TSN Analysis and CPI Protection**
- **Describes SSE activities throughout the Defense Acquisition Life Cycle**
- **<https://acc.dau.mil/dag13>**



# Comprehensive Program Protection Planning across the Lifecycle



- A Program Protection Plan is required for Milestones A, B, C, and FRP/FDD; a draft is required for Pre-EMD.
- PPP is a risk-based process that assesses criticality, threat and supply chain risk, vulnerability, and information assurance risk. Fundamental to this process is a cost-benefit trade-off analysis to identify appropriate countermeasures to mitigate risks to an acceptable level:
  - PPP analysis is conducted iteratively, and results are used to inform Systems Engineering Technical Reviews, as well as other key program events.
  - The PPP analysis becomes more detailed as the requirements are decomposed into system and subsystem specifications
  - Analysis data, and Program Office decisions resulting from the PPP analyses should be documented in the PPP.
  - The results of the PPP analyses are incorporated into Requests for Proposals (RFP) via Statement of Work (SOW) and System Requirements Document (SRD)).



# Policy and Guidance for ASICs



**In applicable systems,\* integrated circuit-related products and services shall be procured from a trusted supplier accredited by the Defense Microelectronics Activity (DMEA) when they are custom-designed, custom-manufactured, or tailored for a specific DoD military end use (generally referred to as application-specific integrated circuits (ASIC)). – DoDI 5200.44**

- **PPP Outline and Guidance on Microelectronics for ASICs**
  - Requires programs to identify all ASICs that require an accredited trusted supplier
  - Requires program to describe how they will make use of accredited trusted suppliers of integrated circuit-related services
- **Defense Acquisition Guidebook (DAG) guidance (Chapter 13)**
  - ASICs meeting policy conditions must be procured from a DMEA accredited trusted supplier implementing a trusted product flow
  - Defense Microelectronics Activity (DMEA) maintains a list of accredited suppliers on its website at <http://www.dmea.osd.mil/trustedic.html>.
  - Critical Design Review (CDR) criteria: Assess manufacturability including the availability of accredited suppliers for secure fabrication of Application-specific integrated circuits (ASICs), Field-programmable gate array (FPGAs), and other programmable devices

**\*Applicable systems:**

- (1) National security systems as defined by section 3542 of title 44, United States Code (U.S.C.) (Reference (l));
- (2) Mission Assurance Category (MAC) I systems, as defined by Reference (j); or
- (3) Other DoD information systems that the DoD Component's acquisition executive or chief information officer determines are critical to the direct fulfillment of military or intelligence missions;



# Policy and Guidance for Other Integrated Circuits



**Control the quality, configuration, and security of software, firmware, hardware, and systems throughout their lifecycles, including components or subcomponents from secondary sources. Employ protections that manage risk in the supply chain for components or subcomponent products and services (e.g., integrated circuits, field-programmable gate arrays (FPGA), printed circuit boards) when they are identifiable (to the supplier) as having a DoD end-use. – DoDI 5200.44**

- **PPP Outline and Guidance on Supply Chain Risk Management:**
  - Requires programs to describe how the program manages supply chain risks to CPI and critical functions and components
- **PPP Outline and Guidance on Trusted Suppliers:**
  - Requires program to describe how the program will make use of accredited trusted suppliers of integrated circuit-related services
- **PPP Outline and Guidance on Counterfeit Prevention:**
  - Requires program to describe counterfeit prevention measures and how the program will mitigate the risk of counterfeit insertion during Operations and Maintenance
- **Defense Acquisition Guidebook (DAG) guidance (Chapter 13)**
  - **Critical Design Review (CDR) Criteria:**
    - Address how the detailed system design includes and appropriately addresses security and SCRM considerations
    - Assess manufacturability including the availability of accredited suppliers for secure fabrication of ASICs, FPGAs, and other programmable devices



# Notional Use Cases and Countermeasures



## Use Cases

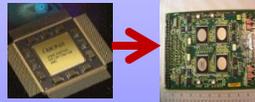
### Use Case 1:

**Custom ASIC** that has a specific DoD military end use



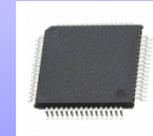
### Use Case 2:

**ASIC in a COTS assembly** that is primarily intended for commercial market



### Use Case 3:

**MOTS/GOTS Integrated Circuit (IC)** that has a DoD end use



## Countermeasures

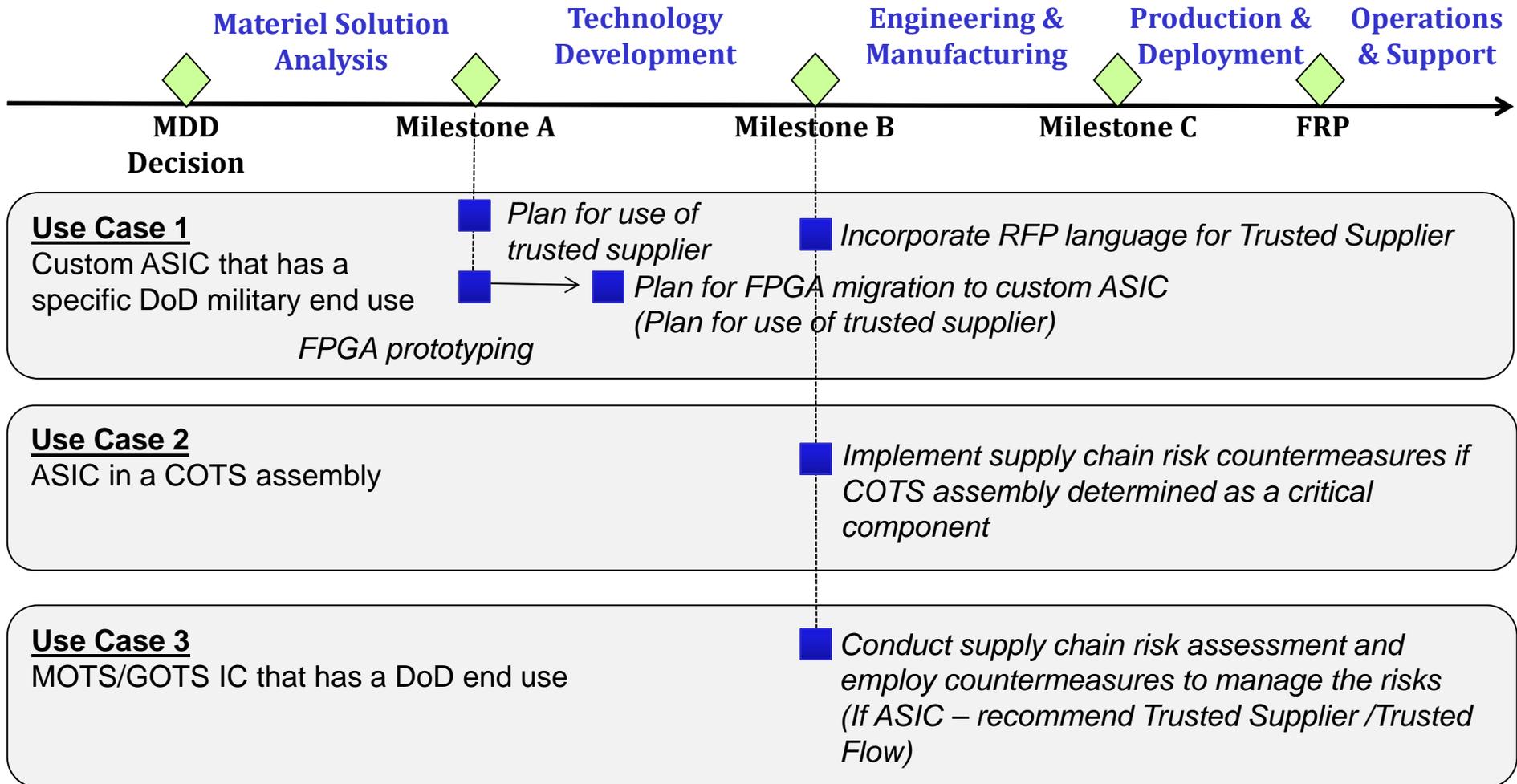
- Use Trusted Supply Flow (Trusted Supplier) for design, mask, fabrication, packaging and testing

- Perform supply chain risk assessment of ASICs if the COTS assembly is determined as a critical component
- Implement SCRM countermeasures commensurate with assessed risk

- Consider source and employment history
- Apply countermeasures commensurate with assessed risk, including enhanced/focused testing
- Use trusted supplier and product flow as applicable, such as FPGA programming services;
- Use DMEA accredited trusted supplier and trusted product flow if ASIC



# Countermeasures Planning



■ Recommended Earliest Decision Point To Apply Mitigation



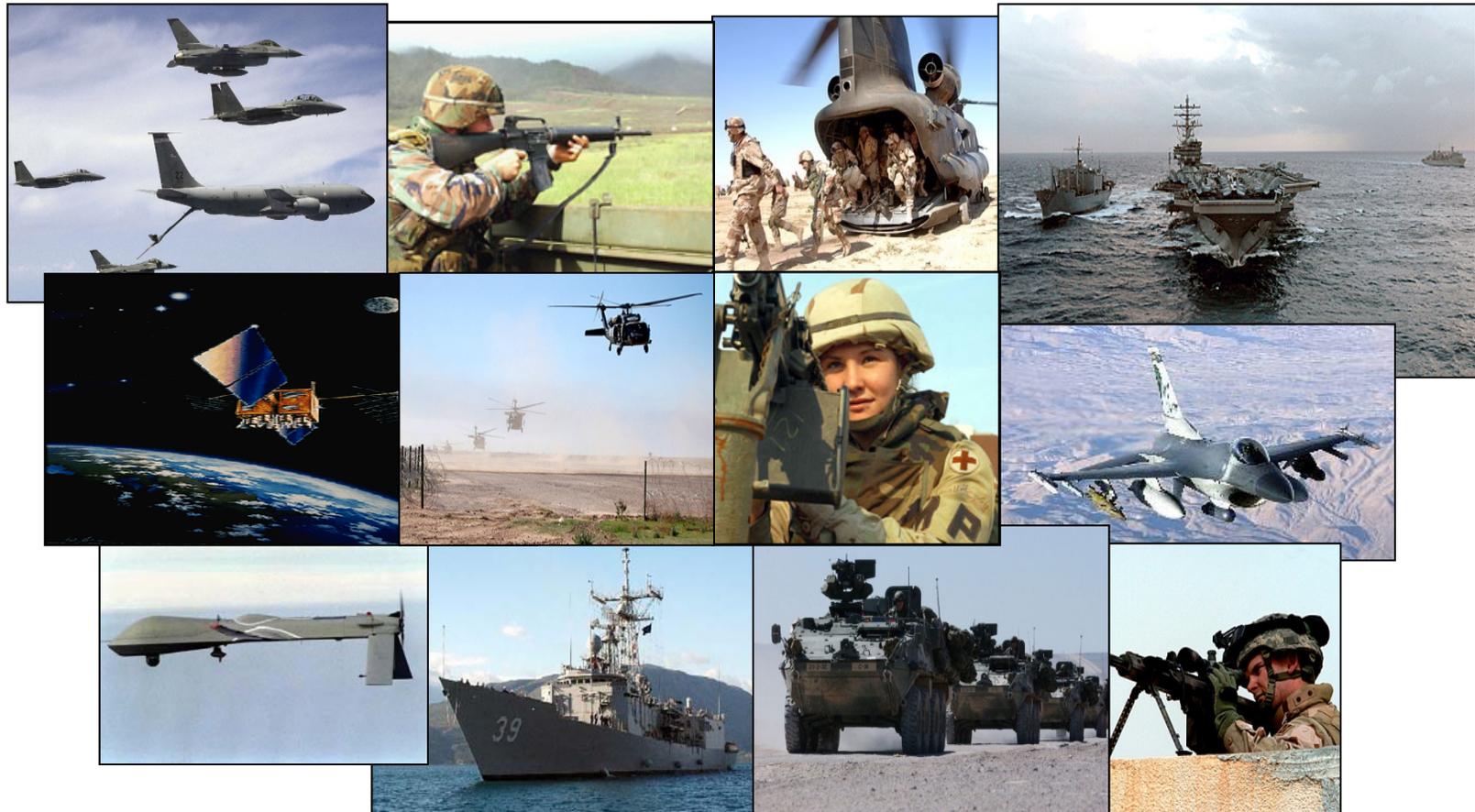
# Industry Partnership



- **Comprehensive Program Protection involves a partnership with that includes DoD, Cleared Defense Contractors (CDCs) and a trusted supplier base**
- **DoD Program Managers and their CDCs rely on trusted suppliers to ensure protection of integrated circuits, critical functions, and critical components**
- **A trusted supplier base is a key element for Program Protection Planning and the DoD Trusted Systems and Networks Strategy**
- **Challenges to Community:**
  - How do we extend ASIC levels of trust to other Integrated Circuit products such as FPGAs?
  - How do we ensure that trust continues during sustainment?



# Systems Engineering: Critical to Program Success



***Innovation, Speed, and Agility***

**<http://www.acq.osd.mil/se>**



# Key Elements of the PPP



Key Sections	Rationale
<b>3.0 CPI and Critical Components (CC)</b> <ul style="list-style-type: none"> <li>Documents output of Research &amp; Tech. Protect and Criticality Analysis</li> <li>Distinguishes between inherited and organic elements</li> </ul>	<b>Focus protection on critical technology, information, and components</b>
<b>4.0 Horizontal Protection</b> <ul style="list-style-type: none"> <li>Assessment of similar CPI on other DoD programs</li> </ul>	<b>Protect technologies across the DoD</b>
<b>5.0 Threats, Vulnerabilities and Countermeasures</b> <ul style="list-style-type: none"> <li>Identifies collection, supply chain, and battlefield threats</li> <li>Documents assessment of vulnerability to threats and mitigating actions</li> </ul>	<b>Acknowledge advanced, persistent threat Assess weaknesses to documented threats and use risk-based mitigations</b>
<b>6.0 Other Plans</b> <ul style="list-style-type: none"> <li>Pointers to related documents (CI Support Plan, TEMP, etc.)</li> </ul>	<b>Reference, not duplicate, key documents</b>
<b>7.0 Residual Risk Assessment</b> <ul style="list-style-type: none"> <li>Document unmitigated risks to CPI and CC compromise</li> </ul>	<b>Document risks program is assuming</b>
<b>8.0 Foreign Involvement</b> <ul style="list-style-type: none"> <li>Identify known and potential foreign military sales, and direct commercial sales</li> <li>Defense Exportability Features (DEF) opportunities</li> </ul>	<b>Drive export realism and prepare for export-specific measures early</b>
<b>9.0 Processes for PM Oversight &amp; Implementation</b>	<b>PM Resources and Implementation Reviews</b>
<b>10.0 Processes for Monitoring &amp; Reporting Loss of CPI and CC</b>	<b>Assess effectiveness of implemented countermeasures</b>
<b>11.0 Costs</b> <ul style="list-style-type: none"> <li>Estimate of implementation costs for CPI and CC protection</li> </ul>	<b>Support cost/benefit assessment of risk mitigations</b>

*The PPP Contains the Information a PM Needs to Effectively Secure the System*