



Cybersecurity and Program Protection

Melinda K. Reed

**Office of the Deputy Assistant Secretary of Defense
for Systems Engineering**

**19th Annual NDIA Systems Engineering Conference
Springfield, Virginia | October 24-27, 2016**



Cybersecurity in Acquisition



- **Acquisition workforce must take responsibility for cybersecurity from the earliest research and technology development through system concept, design, development, test and evaluation, production, fielding, sustainment, and disposal**
- **Scope of program cybersecurity includes:**
 - Program information Data about acquisition, personnel, planning, requirements, design, test data, and support data for the system. Also includes data that alone might not be unclassified or damaging, but in combination with other information could allow an adversary to compromise, counter, clone, or defeat warfighting capability
 - Organizations and Personnel Government program offices, prime and subcontractors, along with manufacturing, testing, depot, and training organizations
 - Networks Government and Government support activities, unclassified and classified networks, contractor unclassified and classified networks, and interfaces among Government and contractor networks
 - Systems and Supporting Systems The system being acquired, system interfaces, and associated training, testing, manufacturing, logistics, maintenance, and other support systems

Cybersecurity is a requirement for all DoD programs



Ensuring Cyber Resilience in Defense Systems



- **Threat:**

- Adversary who seeks to exploit vulnerabilities to:
 - Acquire program and system information;
 - Disrupt or degrade system performance;
 - Obtain or alter US capability

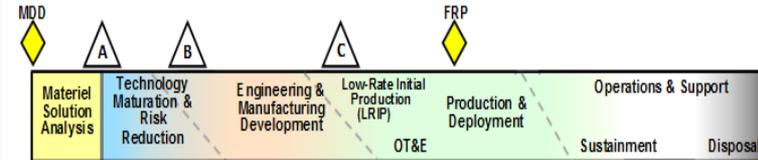
- **Vulnerabilities:**

- Found in programs, organizations, personnel, networks, systems, and supporting systems
- Inherent weaknesses in hardware and software can be used for malicious purposes
- Weaknesses in processes can be used to intentionally insert malicious hardware and software
- Unclassified design information within the supply chain can be aggregated
- US capability that provides a technological advantage can be lost or sold

- **Consequences:**

- Loss of technological advantage
- System impact – corruption and disruption
- Mission impact – capability is countered or unable to fight through

Access points are throughout the acquisition lifecycle...



...and across numerous supply chain entry points

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



Spectrum of 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, electromagnetic 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/software 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.

Reverse Engineering

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

Information Losses

Stolen data provides potential adversaries extraordinary insight into US defense and industrial capabilities and allows them to save time and expense in developing similar capabilities.

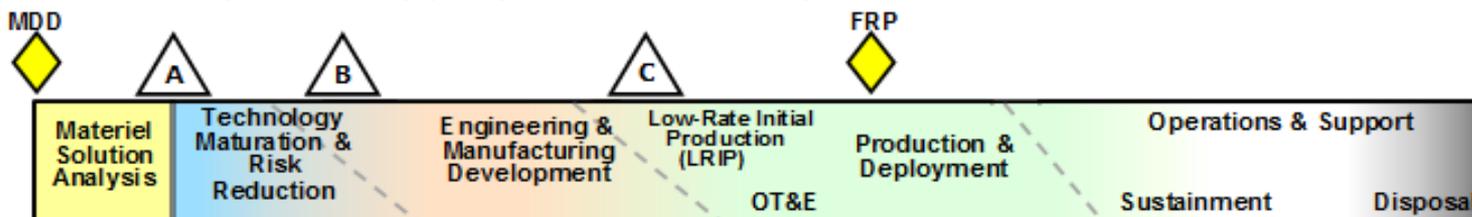
DoD Program Protection focuses on opportunities for malicious actors



Program Protection in DoDI 5000.02 Acquisition Policy



- **DoDI 5000.02 requires Program Managers to employ system security engineering practices and prepare a Program Protection Plan (PPP) to manage the security risks to the program and system elements that are vulnerable and can be exposed to targeting**
 - Critical Program Information
 - Mission-critical functions and critical components
 - Information about the program and within the system
- **PPPs are required at all major milestones**
 - PPPs inform program acquisition strategies, engineering, and test and evaluation plans
 - PMs incorporate appropriate PPP requirements into solicitations





What Are We Protecting?

Program Protection & Cybersecurity

DoDI 5000.02

DoDM 5200.01, Vol. 1-4

DoDM 5200.45

DoDI 8500.01

DoDI 5200.39

DoDI 5200.44

DoDI 5230.24

DoDI 8510.01

Technology

What: A capability element that contributes to the warfighters' technical advantage (CPI)

Key Protection Measure Types:

- Anti-Tamper
- Exportability Features

Goal: Prevent the compromise and loss of CPI

Components

What: Mission-critical functions and components

Key Protection Measure Types:

- Software Assurance
- Hardware Assurance/Trusted Microelectronics
- Supply Chain Risk Management
- Anti-counterfeits

Goal: Protect key mission components from malicious activity

Information

What: Information about the program, system, designs, processes, capabilities and end-items

Key Protection Measure Types:

- Classification
- Export Controls
- Information Security

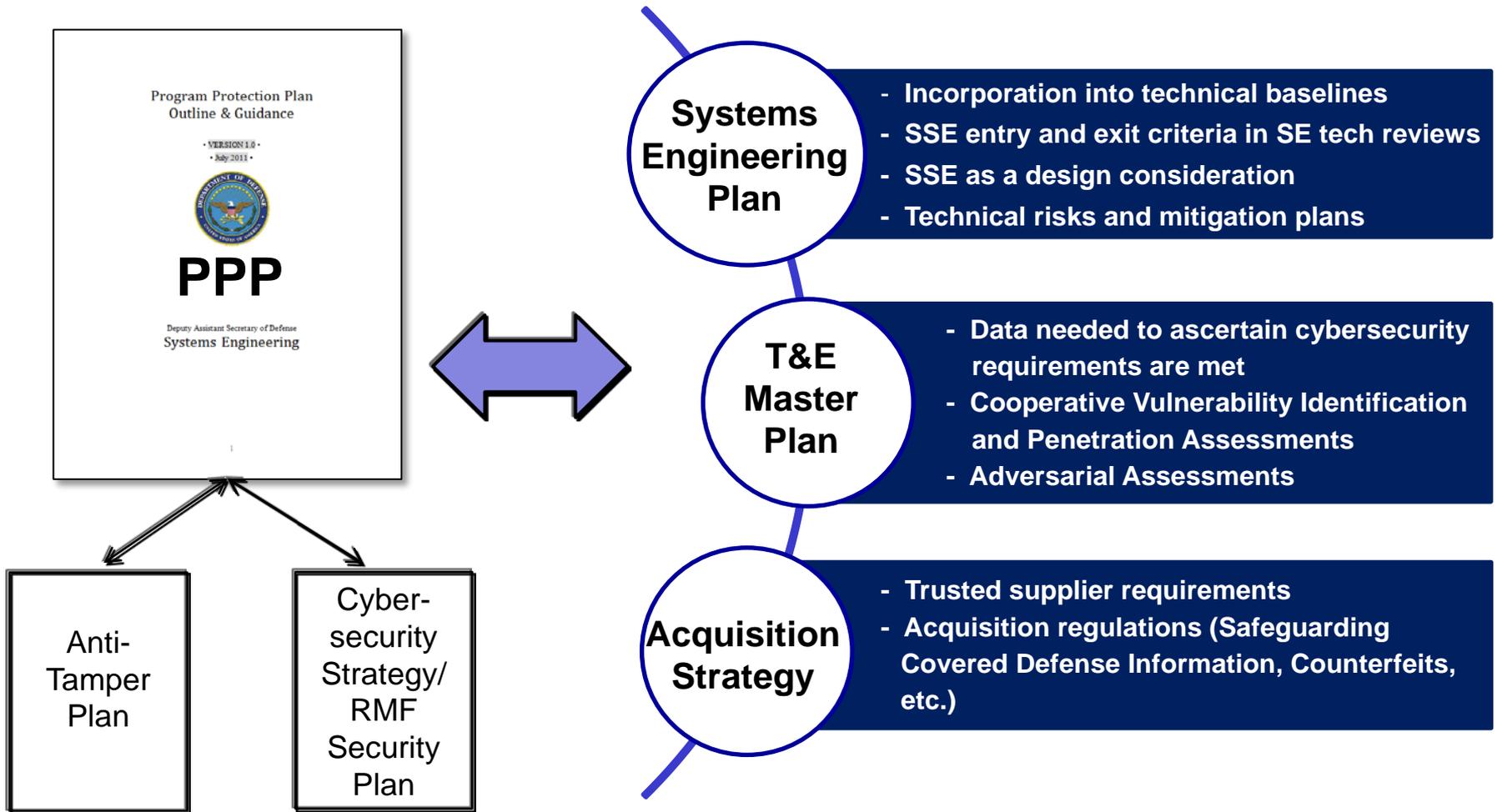
Goal: Ensure key system and program data is protected from adversary collection

Protecting Warfighting Capability Throughout the Lifecycle

Policies, guidance and white papers are found at our initiatives site: http://www.acq.osd.mil/se/initiatives/init_pp-sse.html



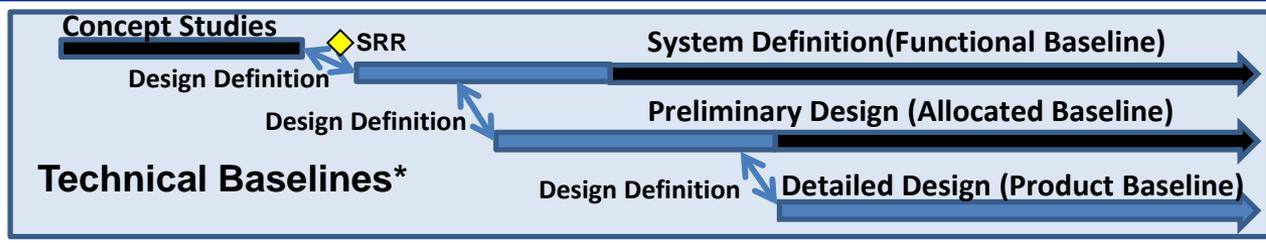
Program Protection Relationship to Other Formal Acquisition Activities



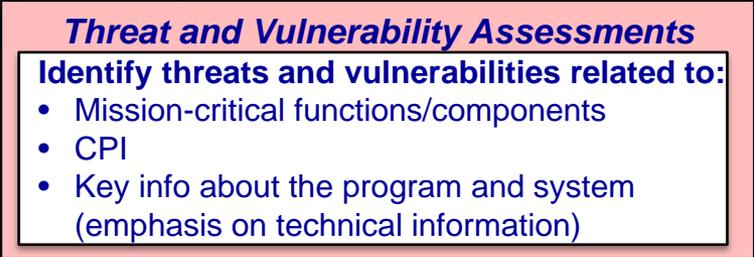
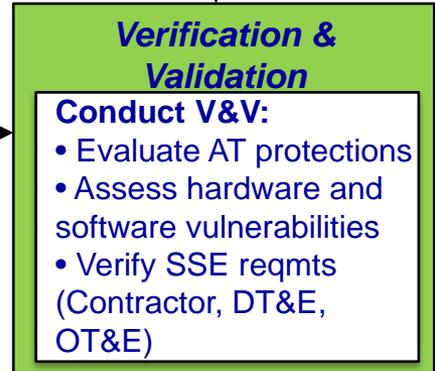
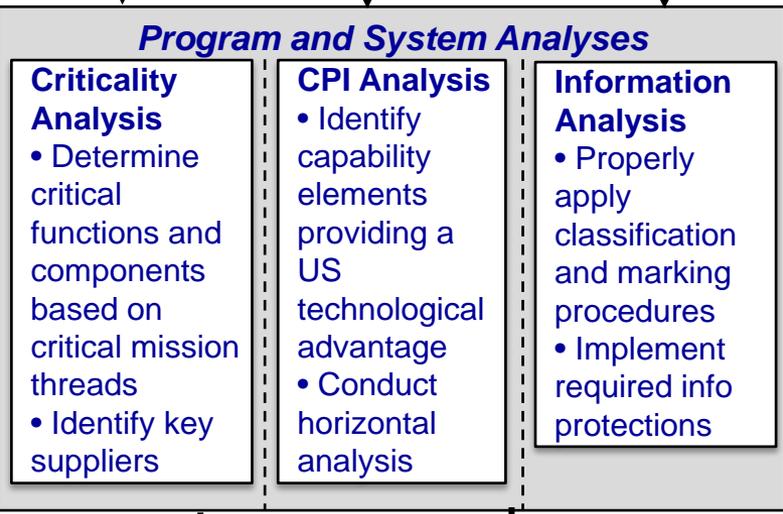
Tailored to specific program situations



Systems Security Engineering Activity Overview



- Protections are identified and integrated into technical baselines
- Analyses are iteratively informed by and informing the design
- Results are documented in the PPP





Contract Regulation for Safeguarding Covered Defense Information



DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting:

- 2nd interim rule published December 30, 2015, to provide contractors with additional time to implement NIST 800-171 security requirements

Purpose:

- Establish minimum requirements for contractors and subcontractors to safeguard DoD unclassified covered defense information and report cyber incidents on their contractor owned and operated information systems

Requires Contractors to:

- Flow down only to Subcontractors where their efforts will involve covered defense information or where they will provide operationally critical support
- Fully comply with security requirements in the NIST SP 800-171, "Protecting Controlled Unclassified Information in *Nonfederal* Information Systems and Organizations" NLT Dec 31, 2017
- Report cyber incident and compromises affecting covered defense information
- Submit malware that they are able to discover and isolate in connection with a reported cyber incident
- Support DoD damage assessment as needed

Final rule anticipated to be published in Fall 2016

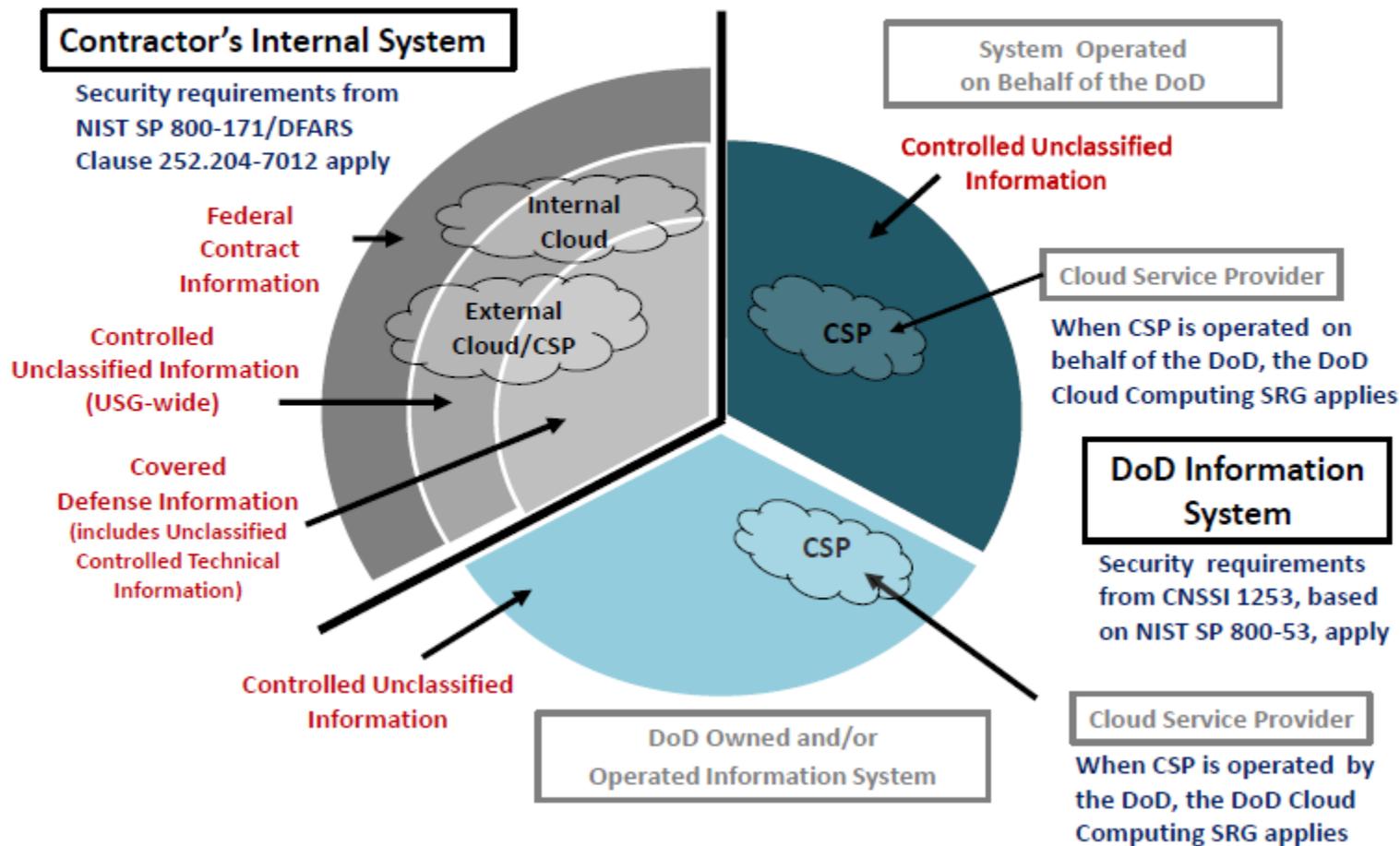


Safeguarding Covered Defense Information Environment



Protecting the DoD's Unclassified Information...

Information System Security Requirements





Protection Planning in Solicitations



- **PMs must ensure that appropriate cybersecurity and system security requirements are incorporated into contracts**
 - Federal Acquisition Regulations
 - Defense Federal Acquisition Regulation Supplement
 - Statement of Work/Performance Work Statements
 - System Specifications
 - Contract Data Requirements Lists

The PM's Program Protection Planning activities play a Key Role in informing the Request for Proposal



Incorporating Program Protection into Acquisition Workforce Training



- **ACQ 160: Program Protection Overview**
 - Distance learning (online); ~3 days
 - Provides an overview of program protection concepts, policy and processes
 - Intended for the entire Acquisition Workforce, with focus on ENG and PM
 - **Course deployed on DAU website on 15 Aug 2016**
- **ENG 260: Program Protection Practitioner Course (est. deployment Summer 2017)**
 - Hybrid (online and in-class); ~1 week
 - Intended for Systems Engineers and System Security Engineers
 - Focuses on application of program protection concepts and processes
- **Future: Provide topic-specific CLMs**
 - DEF, AT, SwA, SCRM, etc.



Effective program protection planning requires qualified, trained personnel



Summary

- **Cybersecurity and related Program Protection is an essential element of acquisition, engineering, test, and sustainment activities**
 - Establishing security as a fundamental discipline of systems engineering
- **DoD continues to refine guidance for a risk-based cost effective approach protect programs and systems**
 - Ensuring that cybersecurity and related program protection activities are addressed as part of systems engineering, test, and sustainment activities
 - Incorporating cybersecurity and related program protection requirements and processes into contracts
 - Working with industry and standards groups to synergize methodologies
- **Industry, academia and government play an important role by:**
 - Investing in research and processes to protect program and system information that extends to the supply chain
 - Developing design methods, standards and tools to enable policy implementation
 - Educating and training their engineering workforce on the importance of their involvement



Systems Engineering: Critical to Defense Acquisition



PP/SSE Initiatives Webpage
http://www.acq.osd.mil/se/initiatives/init_pp-sse.html

JFAC Portal
<https://jfac.army.mil/> (CAC-enabled)



For Additional Information



Melinda Reed

ODASD, Systems Engineering
571-372-6562 | Melinda.K.Reed4.civ@mail.mil

Edward Chatters

Engility Corporation
571-372-6490 | Edward.P.Chatters.ctr@mail.mil



Unclassified Information Regulation Landscape



Protecting the DoD's Unclassified Information... Defining the Landscape

Types of Unclassified Information Systems

- Contractor's Internal Information System
- DoD Information System
 - DoD Owned and/or Operated Information System
 - System Operated on Behalf of the DoD

Types of Unclassified Information

- Covered Defense Information (to include Unclassified Controlled Technical Information)
 - *August 26, 2015 and December 30, 2015, DFARS Case 2013-D018, Network Penetration Reporting and Contracting for Cloud Services (interim rule) (80 FR 51739 and 80 FR 81472)*
- Controlled Unclassified Information (CUI)
 - *November 4, 2010, Executive Order 13556, Controlled Unclassified Information, and May 8, 2015, 32 CFR 2002, Proposed CUI Federal Regulation*
- Federal Contract Information
 - *May 16, 2016, FAR Case 2011-020, Basic Safeguarding of Contractor Information Systems (81 FR 30439)*





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



DoDI 5200.39 Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)

- Assigns responsibility for Counterintelligence, Security, and System Engineering support for the ID and protection of CPI
- Rescoped definition 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



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



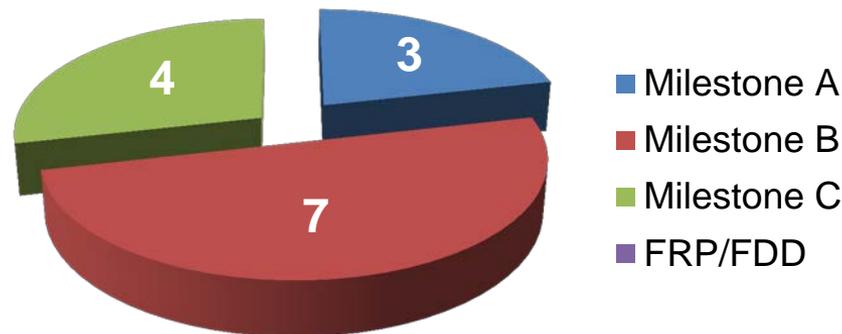
PPP Approval Statistics Since Outline and Guidance Signed



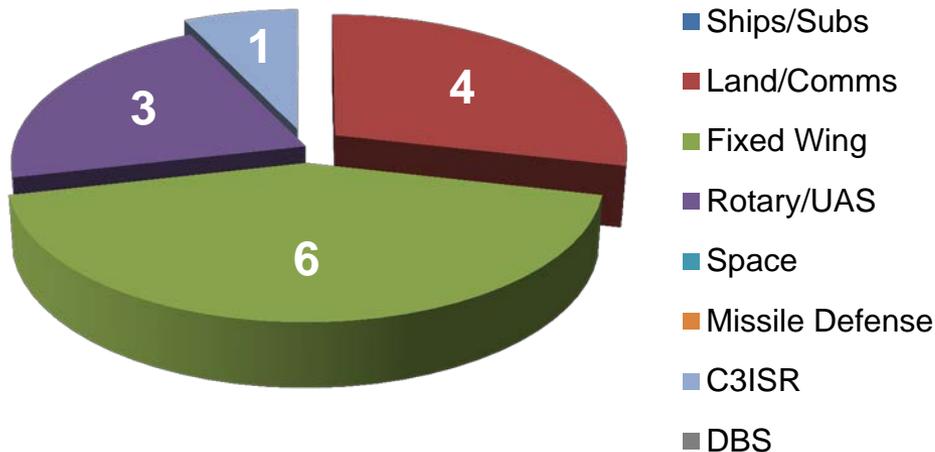
76 PPPs Approved

FY 2011 – 7	FY 2014 – 18
FY 2012 – 5	FY 2015 – 14
FY 2013 – 18	FY 2016 – 14

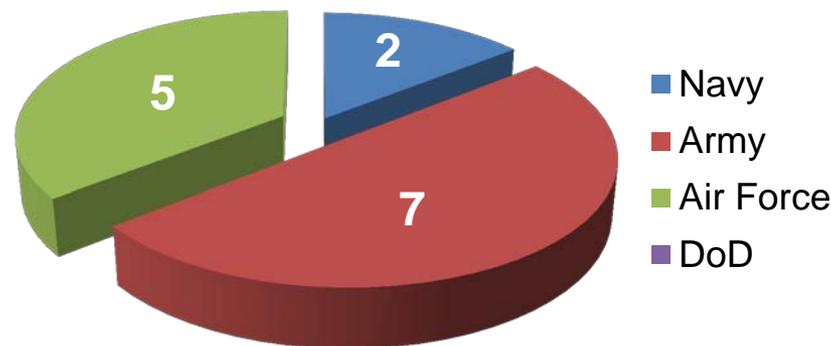
FY16 PPPs by Milestone



FY16 PPPs by Domain



FY16 PPPs by Service



Engaged with and Tracked 55 Programs During FY 2016