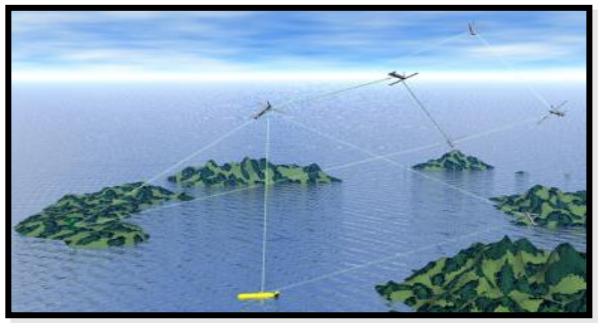
Resilient Systems Directorate Overview

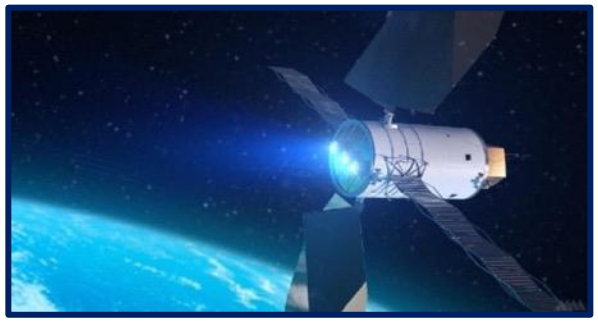
Ms. Melinda Reed
Director, Resilient Systems
Office of the Under Secretary of Defense
for Research and Engineering

National Defense Industrial Association
Systems Engineering Division Meeting
October 21, 2020

Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) Mission

- **Ensure Technological Superiority for the U.S. Military**
  - Set the technical direction for the Department of Defense (DoD)
  - Champion and pursue new capabilities, concepts, and prototyping activities throughout DoD research and development enterprise
- **Bolster Modernization**
  - Pilot new acquisition pathways and concepts of operation
  - Accelerate capabilities to the warfighter





DDR&E/R&T Strategic Technology Protection & Exploitation

Deputy Director
Strategic Technology Protection & Exploitation (STP&E)
Dr. Robert Irie

Acting D, Maintaining Technology Advantage
Mr. Kristopher Gardner

Maintain Leadership in Critical Technology Modernization Areas

- Implement Department Research Security agenda
- Update DoD and Govt-wide procedures to strengthen U.S. research enterprise
- Mitigate exploitation in academia, labs, FFRDCs, UARCs and industry
- Integrate Allies and Partners into research security actions countering strategic competitors' activities
- Focus security, counterintelligence, and law enforcement actions to deter adversaries

D, Resilient Systems
Ms. Melinda Reed

Foster Assured Resilient Missions, Systems and Components

- Set the technical and policy direction for technology and program protection
- Advance DoD capability/capacity to evaluate and mitigate software component vulnerabilities
- Modernize secure cyber-resilient weapons, engineering methods, and workforce competency

D, Technology and Manufacturing Industrial Base
Mr. Robert Gold

Advance Domestic Innovation Base to Deliver Modernization Goals

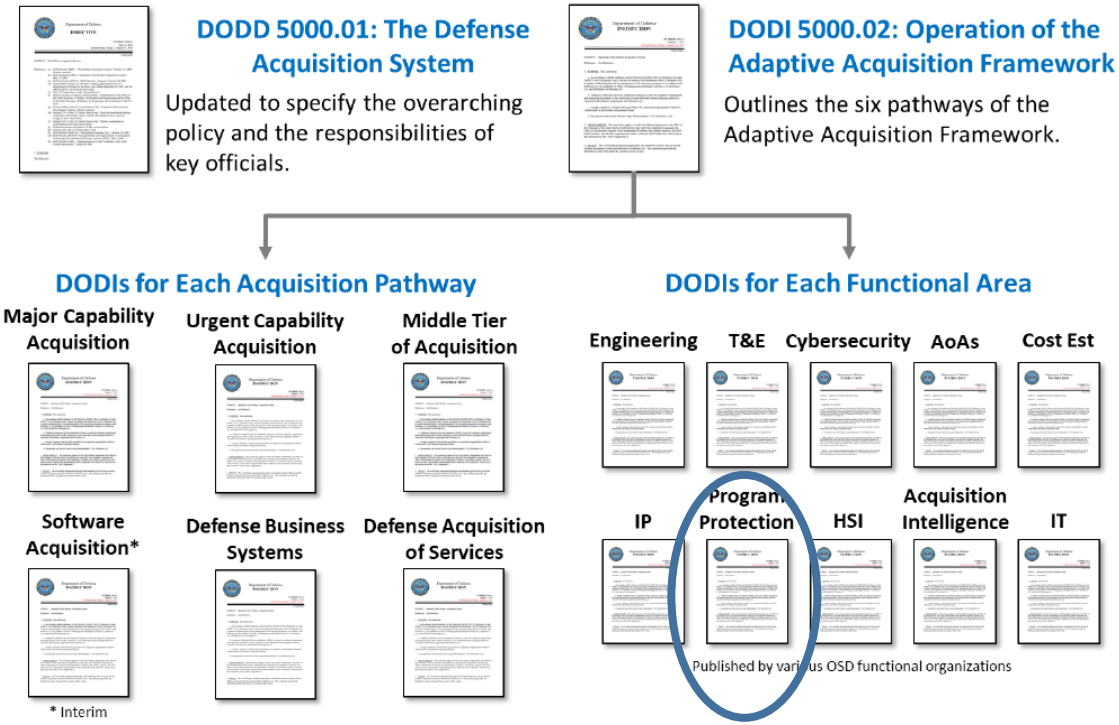
- Assess and monitor emerging technology, workforce, engineering, test, & infrastructure base
- Facilitate USG mechanisms and tools to close gaps, foster enabling domestic technology development and manufacturing capability, and counter strategic competitor actions
- Manage the OSD Manufacturing Technology program and Manufacturing Innovation Institutes

MISSION: Promote and protect technology advantage and counter unwanted technology transfer to ensure warfighter dominance through superior, assured, and resilient systems, and a healthy viable national security innovation base.

Transformation of Acquisition Policy *

DoD 5000 Series Re-write: What Changes?

Revised DoDI 5000.02 will include an Adaptive Acquisition Framework (AAF) with 6 tailorable acquisition pathways and DoDIs for each functional area.



*https://www.acq.osd.mil/ae/assets/docs/Transforming%20Defense%20Acq%20Policy%20(15Jan2020).pdf

Technology and Program Protection Planning Across the Lifecycle

Technology Modernization Priorities

- 5G Network Technology
- Autonomy
- Biotechnology
- Cyber
- Directed Energy
- Fully Networked Command, Control, and Communications
- Hypersonics
- Machine Learning / Artificial Intelligence
- Microelectronics
- Quantum Science
- Space

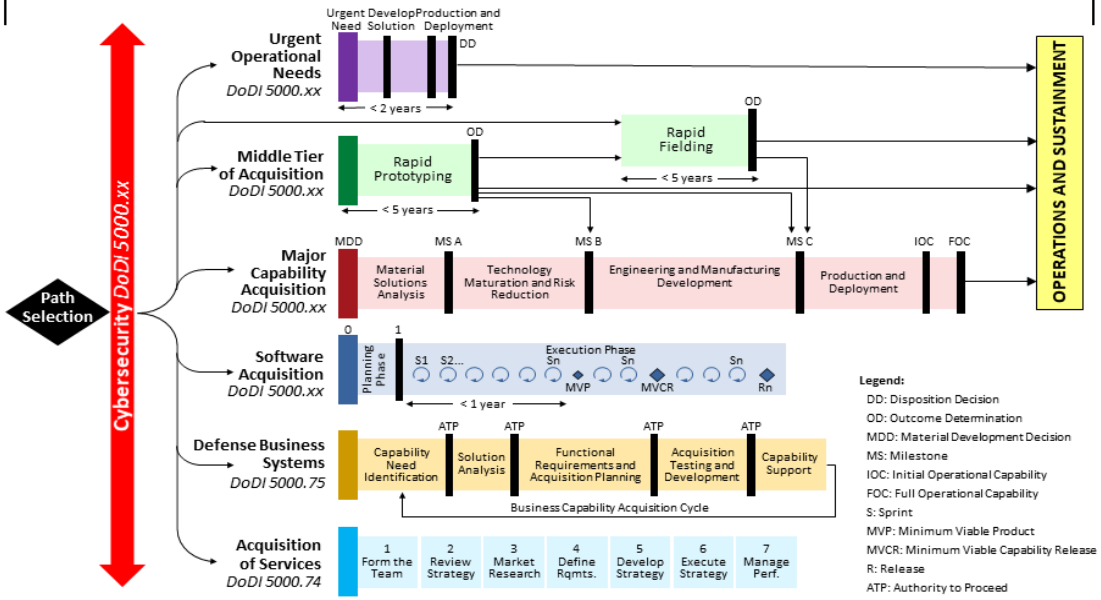
Adaptive Acquisition Framework

Enable Execution at the Speed of Relevance

Tenets of the Defense Acquisition System

1. Simplify Acquisition Policy
2. Tailor Acquisition Approaches
3. Empower Program Managers
4. Data Driven Analysis
5. Active Risk Management
6. Emphasize Sustainment

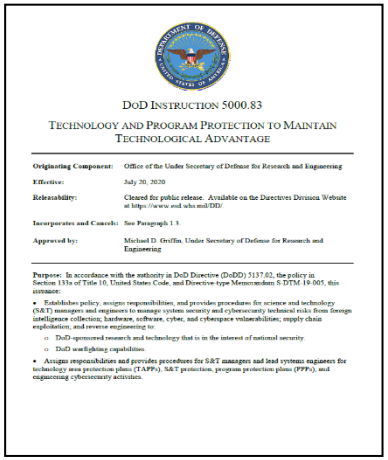
DoDD 5000.01: *The Defense Acquisition System*
DoDI 5000.02: *Operation of the Adaptive Acquisition Framework*



S&T Protection | **Program Protection**

Technology Area Protection Plans for DoD Modernization Priorities

Department of Defense Instruction 5000.83



DoD Instruction 5000.83

Technology and Program Protection to Maintain Technological Advantage

Originating Component: Office of the Under Secretary of Defense for Research and Engineering

Effective: July 20, 2020

Releasability: Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.

Incorporates and Cancels: See Paragraph 1.3.

Approved by: Michael D. Griffin, Under Secretary of Defense for Research and Engineering

Purpose: In accordance with the authority in DoD Directive (DoDD) 5137.02, the policy in Section 133a of Title 10, United States Code, and Directive-type Memorandum 8-DTM-19-005, this instruction:

- Establishes policy, assigns responsibilities, and provides procedures for science and technology (S&T) managers and engineers to manage system security and cybersecurity technical risks from foreign intelligence collection; hardware, software, cyber, and cyberspace vulnerabilities; supply chain exploitation; and reverse engineering to:
  - DoD-sponsored research and technology that is in the interest of national security.
  - DoD warfighting capabilities.
- Assigns responsibilities and provides procedures for S&T managers and lead systems engineers for technology area protection plans (TAPPs), S&T protection, program protection plans (PPPs), and engineering cybersecurity activities.

- Establishes policy, assigns responsibilities, and provides procedures for DoD science and technology managers and engineers to mitigate risks and protect critical U.S. research, military technologies, and programs
- Contributes to a National Defense Strategy (NDS) line of effort (increasing lethality) through promotion and implementation of enhanced technology protection across the DoD enterprise
- The Department of Defense Instruction (DoDI) recommends activities for DoD S&T managers and engineers to mitigate threats to U.S. technology and programs, including:

- Safeguarding classified and unclassified Controlled Technical Information
- Supervising DoD-sponsored research involving joint ventures, academic collaborations, and cooperative research partnerships
- Designing systems for security and cyber resiliency
- Protecting against cyberattacks
- Protecting fielded systems from changing threat environments
- Enhancing protection for critical programs and technologies through Technology Area Protection Plans (TAPPs), S&T protection plans, and Program Protection Plans (PPPs)

- Released 20 July 2020; available on https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500083p.pdf?ver=2020-07-20-150345-930/

Technology, Program Protection & Cybersecurity Related Policies

Technology

Key Protection Activities:

- Export Control
- Anti-Tamper
- Defense Exportability Features
- DoD Horizontal Protection Guide
- Acquisition Security Database

Goal: Prevent compromise or loss of critical technology transfer

- **DoDI 5200.39 Critical Program Information**
- **DoDD 5200.47E Anti-Tamper**
- **DFARS 225.7901 Export-controlled items**

Mission Components

Key Protection Activities:

- Software Assurance
- Hardware Assurance
- Supply Chain Risk Management
- Anti-counterfeits
- Joint Federated Assurance Center

Goal: Protect mission-critical components (hardware, software) from malicious exploitation

- **DoDI 5200.44 Trusted Systems & Networks**
- **PL 113-66 Sec 937 (FY14 NDAA) JFAC**
- **DFARS 239.73 Requirements for information relating to supply chain risk**
- **NDAA FY11 Sec 806; Requirements for Information Relating to Supply Chain Risk**
- **NDAA FY18 Sec 1659. Supply Chain Risk Management of Critical Missions**
- **NDAA FY20 Sec 224, Trusted Supply Chain Standards**
- **NDAA FY17 Sec 231 DoDI Microelectronics**

Information

Key Protection Activities:

- Classification
- Information Security
- Cybersecurity Protections and Technology Solutions
- Joint Acquisition Protection & Exploitation Cell (JAPEC)
- Damage Assessment Management

Goal: Safeguard system and technical data from adversary collection and disruption

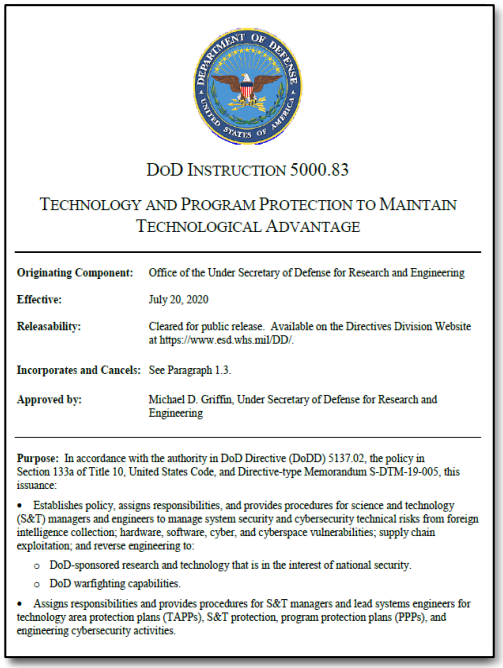
- **DoDI 5230.24 Distribution Statements on Technical Information**
- **DoDI 5200.48 Controlled Unclassified Information**
- **DFARS 252.204-7012 Safeguarding covered defense information and cyber incident reporting (includes requirement to implement NIST SP800-171)**
- **DCMA NIST SP 800-171 Strategic Assessments**
- **32 CFR 2002: Controlled Unclassified Information**

Goal: Ensure warfighter dominance through superior, assured, and resilient systems

Alignment to National Defense Strategy

Technology and Program Protection	• Assigns responsibilities for S&T managers and engineers • OUSD(R&E) monitors process, delegates responsibility to greatest extent practicable; approves acquisition categories (ACAT) 1D Program Protection Plans • Links to Pathways, Engineering, Cybersecurity in the Acquisition System, Test and Evaluation, and Sustainment
Activities to Mitigate Adversary Threats	• Includes responsibilities for DoD-sponsored research, prior to Materiel Development Decision (MDD) • Reinforces best practices for risk informed technical and engineering mitigations • Implements technical information, hardware assurance, software assurance, anti tamper, cyber resilient security engineering methods and level of assurance to achieve protection and cyber objectives • Refreshed periodically throughout the program lifecycle
Technology Modernization Priorities	• Establishes TAPP for modernization priorities • Establishes S&T Protection activities • Enhanced protection for critical programs and technologies
Tailored Program Protection for Acquisition Pathways	• Enables tailoring to pathway focus areas • Determine protection planning and implementation risks as part of the design and technical risk assessment process • Ensure operator is informed of operational risks when system is fielded

Technology and Program Protection to Maintain Technological Advantage – DoDI 5000.83



DoD Instruction 5000.83

Technology and Program Protection to Maintain Technological Advantage

Originating Component:	Office of the Under Secretary of Defense for Research and Engineering
Effective:	July 20, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Incorporates and Cancels:	See Paragraph 1.3.
Approved by:	Michael D. Griffin, Under Secretary of Defense for Research and Engineering

Purpose: In accordance with the authority in DoD Directive (DoDD) 5137.02, the policy in Section 133a of Title 10, United States Code, and Directive-type Memorandum S-DTM-19-005, this issuance:

- Establishes policy, assigns responsibilities, and provides procedures for science and technology (S&T) managers and engineers to manage system security and cybersecurity technical risks from foreign intelligence collection; hardware, software, cyber, and cyberspace vulnerabilities; supply chain exploitation; and reverse engineering to:
  - DoD-sponsored research and technology that is in the interest of national security.
  - DoD warfighting capabilities.
- Assigns responsibilities and provides procedures for S&T managers and lead systems engineers for technology area protection plans (TAPPs), S&T protection, program protection plans (PPPs), and engineering cybersecurity activities.

- **Safeguard information**
- **Control DoD-sponsored research**
- **Design for security and cyber resiliency**
- **Protect the system against cyber attacks from enabling and supporting systems**
- **Protect fielded systems**
- **Enhance protection for critical programs and technologies**

Technology Area Protection Plan (TAPP)

- OUSD(R&E) identifies broad technology elements to protect that are central to accelerating Warfighter capabilities in key technology areas across the Department
- Set boundaries on what should be communicated by stakeholder groups for protection purposes

Science and Technology (S&T) Protection Plan

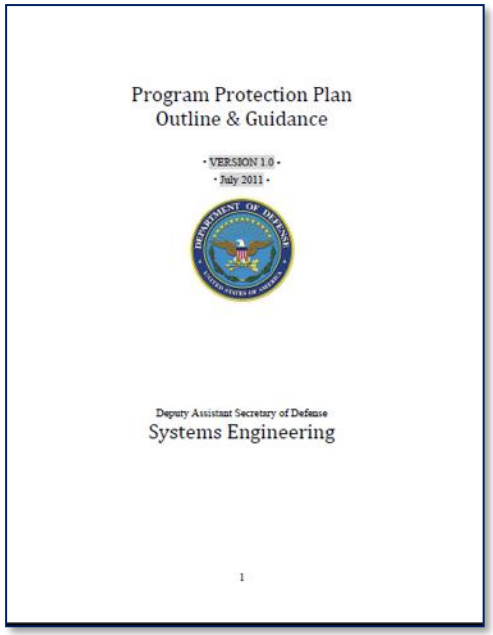
- Management tool to guide protection activities for S&T Investments at DoD Component-level
- Implement risk-based protection measures to reduce compromise or loss to competitor nations through transition to acquisition

Program Protection Plan (PPP)

- Acquisition management tool to guide the systems security engineering, to include cyber resilient engineering, activities across the life cycle
- Informed by TAPP and S&T Protection Plans

Manage risk of adversarial exploitation and compromise beginning with early S&T and continues through the Acquisition lifecycle

Implementation: Program Protection Planning Update



Modernize the PPP Outline and Guidance

- Policy Updates
- Acquisition Regulations
- Standards
- Lessons Learned

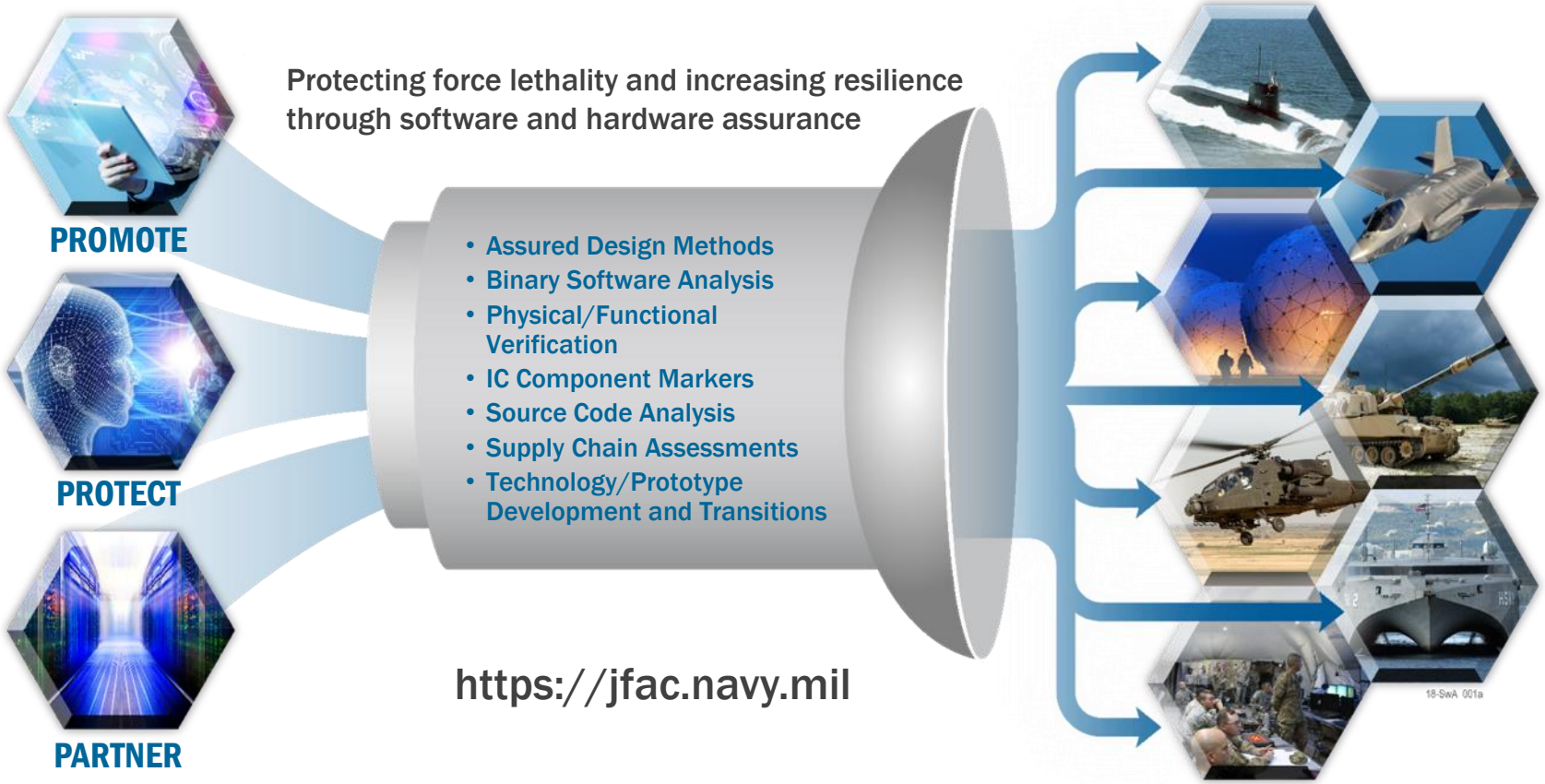
Concerted effort to enable consistent tailored implementation

- *Scheduling virtual roadshows to provide training on implementation of DoDI 5000.83*

- *Updates to Defense Acquisition University (DAU) S&T managers and engineering education and training for technology and program protection will be informed by R&E-led Engineering Workforce Task Force*

Collaboration with stakeholders is forthcoming

Implementation: Joint Federated Assurance Center



- Federated laboratory capability of expertise and tools for vulnerability detection and analysis
- Support program offices with software and hardware assurance expertise and capabilities
- Stakeholders - Army, Navy, Air Force, National Security Agency (NSA), Defense Microelectronics Activity (DMEA), OUSD(R&E), DoD CIO, Defense Information Systems Agency (DISA), National Reconnaissance Office (NRO), Missile Defense Agency (MDA), OUSD(A&S)

Summary

- **DoDI 5000.83 establishes roles and responsibilities for the S&T manager and the engineering workforce**
  - **Updates to guidance, standards, education and training are pending to make more consistent implementation**
- **Improve the efficiency and effectiveness of weapon systems engineering practice**
- **Increase consistency and repeatability of resilient engineering methods and standards**
- **Improve the communication between government, industry, and operational stakeholders**

Customer-Focused: Outcome-Based

Questions