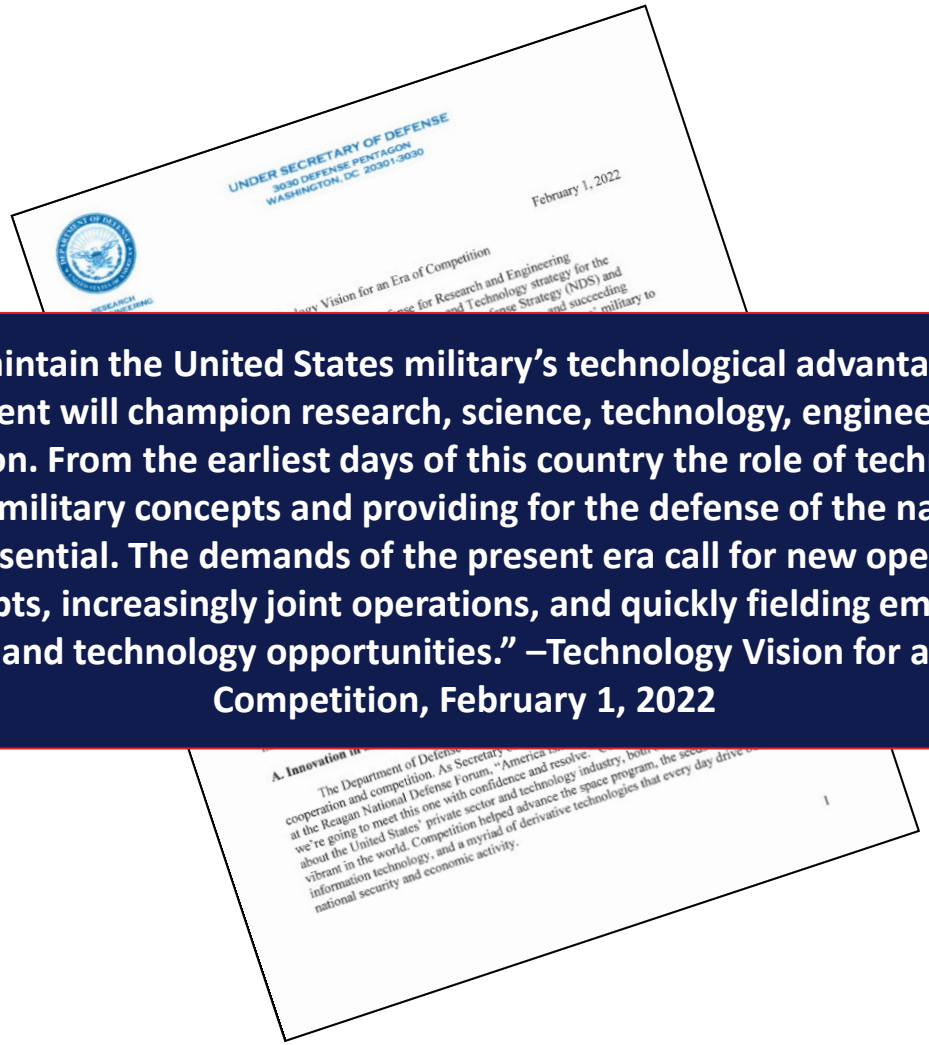
USD(R&E)

Program Protection and Secure Cyber Resilient Engineering Initiatives

Presented to NDIA Systems and Mission Engineering Conference
Orlando, Florida
November 2022

Melinda Reed
Director, Systems Security
Office of Under Secretary of Defense for
Research and Engineering
Science and Technology Program Protection

Our Mission


UNDER SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

February 1, 2022

Technology Vision for an Era of Competition

A. Innovation

The Department of Defense

cooperation and competition. As Secretary

at the Reagan National Defense Forum, "America

we're going to meet this one with confidence and resolve.

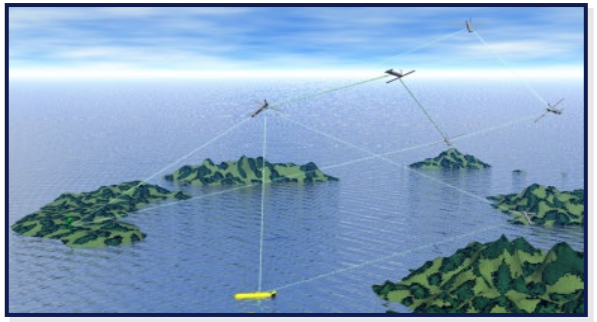
about the United States' private sector and technology industry, both

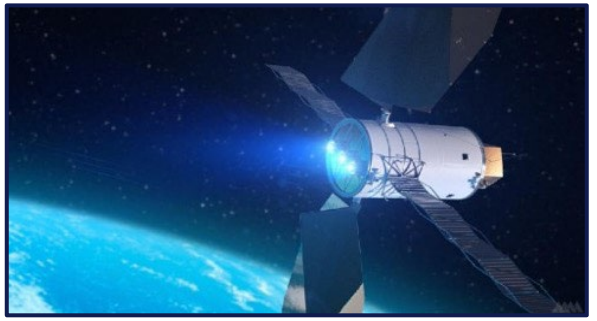
vibrant in the world. Competition helped advance the space program, the

information technology, and a myriad of derivative technologies that every day drive

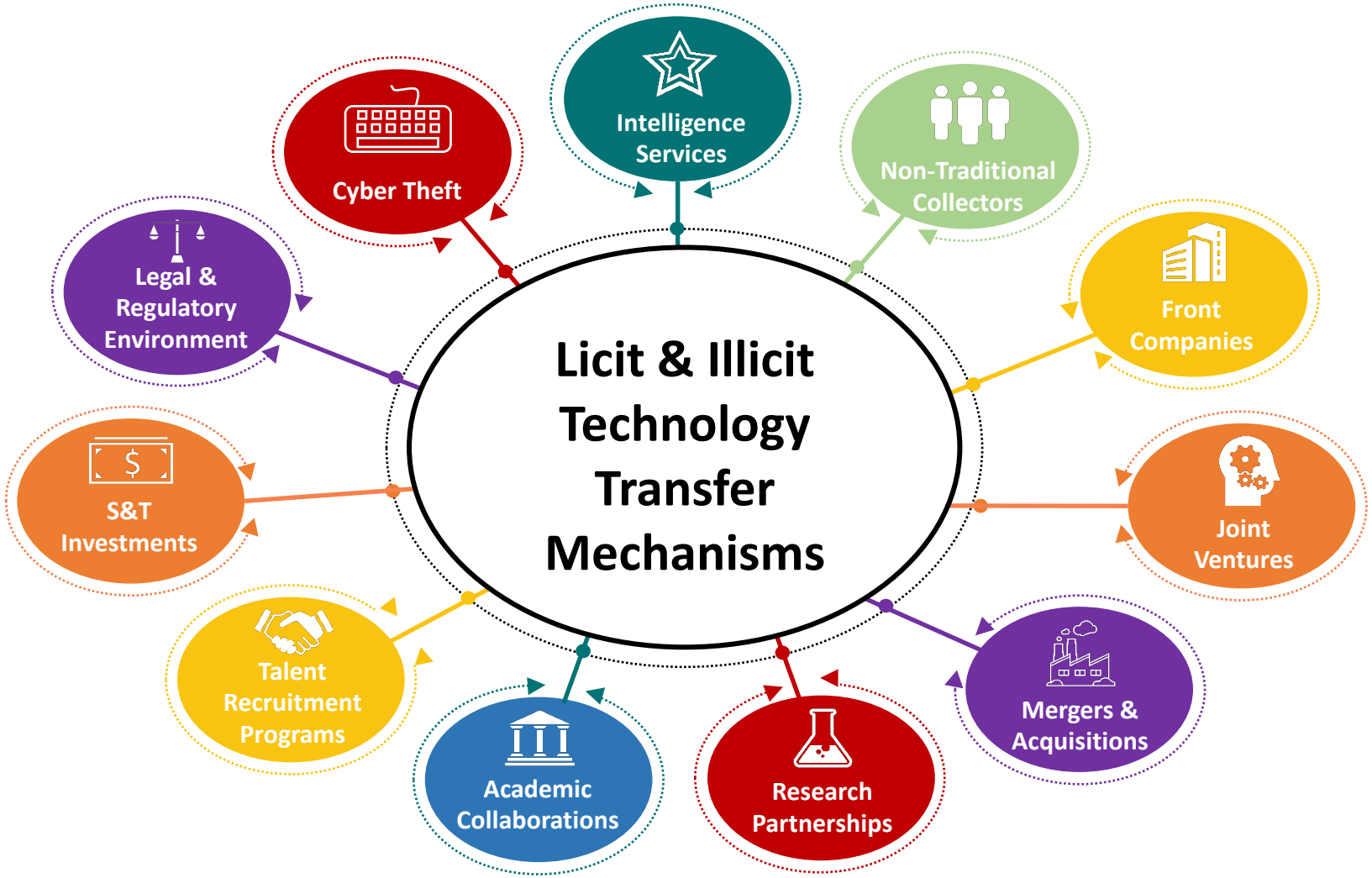
national security and economic activity.

"To maintain the United States military's technological advantage, the Department will champion research, science, technology, engineering, and innovation. From the earliest days of this country the role of technology in shaping military concepts and providing for the defense of the nation has been essential. The demands of the present era call for new operational concepts, increasingly joint operations, and quickly fielding emerging science and technology opportunities." –Technology Vision for an Era of Competition, February 1, 2022





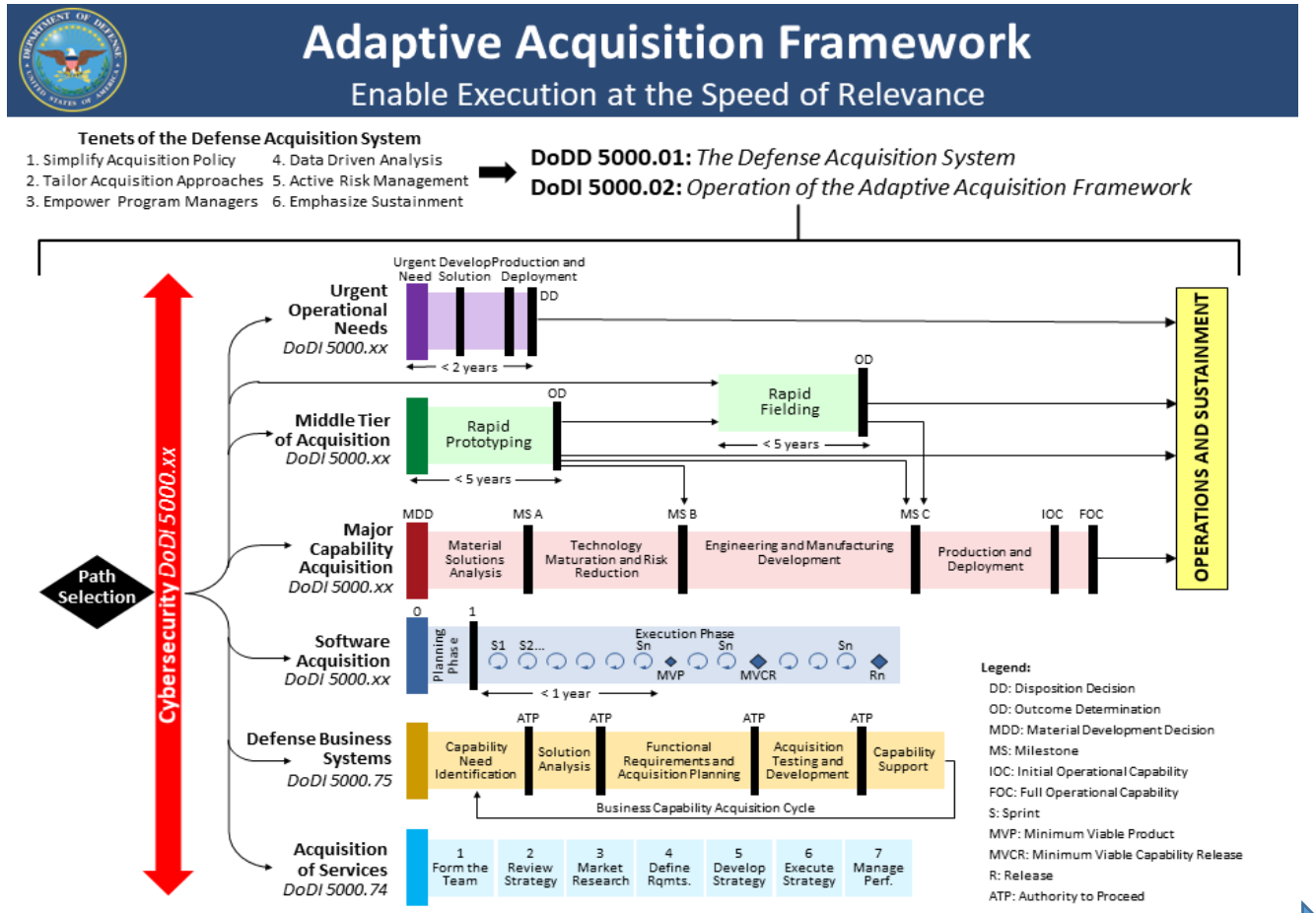
Threats to Our Mission



Technology and Program Protection Planning Across the Lifecycle

Critical Technology Areas

- Advanced Computing and Software
- Advanced Materials
- Integrated Sensing and Cyber
- Integrated Network Systems-of-Systems
- Trusted AI and Autonomy
- Biotechnology
- Future Generation Wireless Technology (FutureG)
- Directed Energy
- Human-Machine Interfaces
- Hypersonics
- Quantum Science
- Renewable Energy Generation and Storage
- Microelectronics
- Space Technology

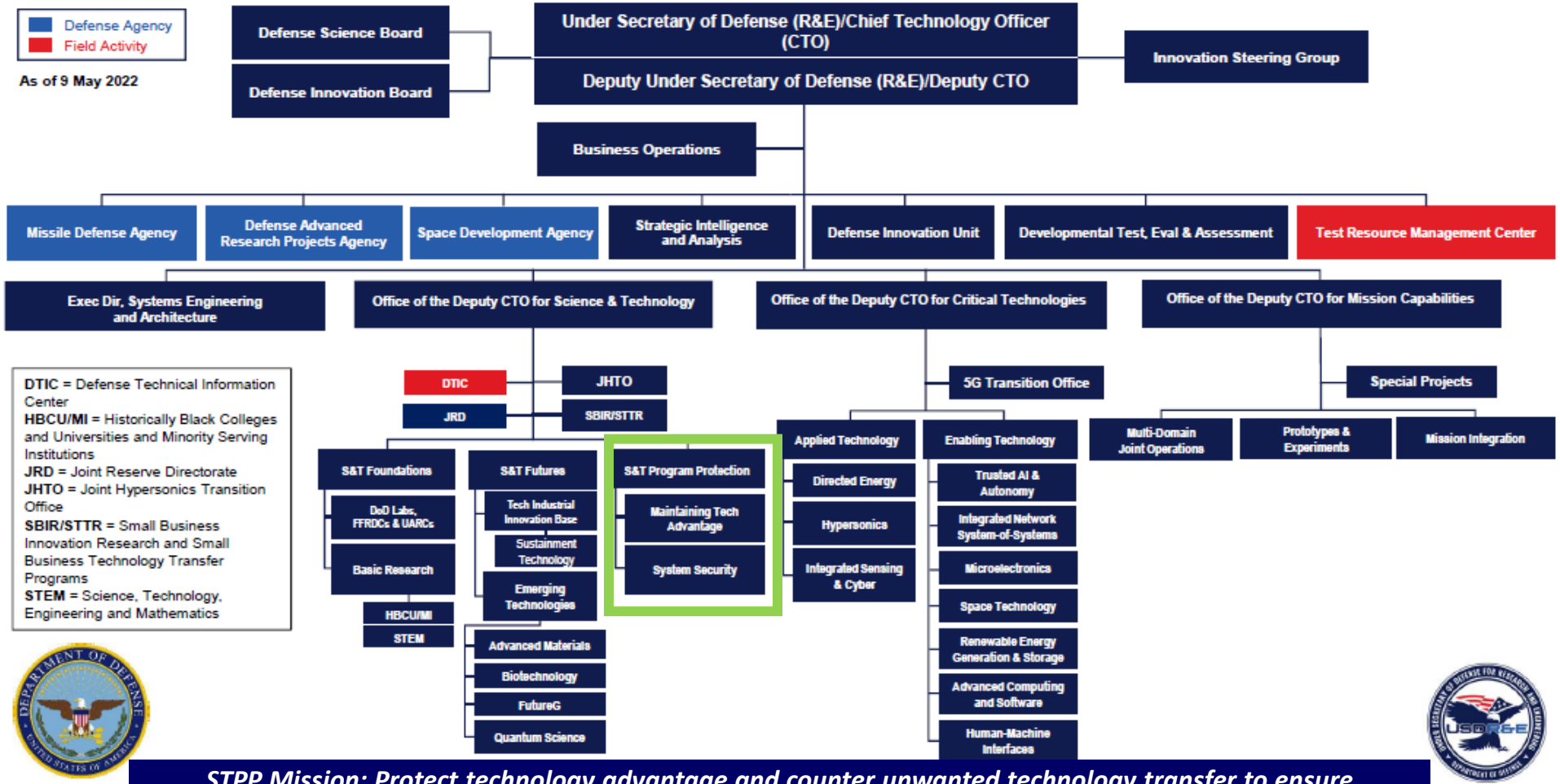


S&T Protection

Program Protection

Technology Area Protection Plans for DoD Critical Technology Areas

Office of the Under Secretary of Defense for Research and Engineering Organization



STPP Mission: Protect technology advantage and counter unwanted technology transfer to ensure warfighter dominance through assured, secure and resilient systems and a healthy viable national security innovation base

Systems Security Mission and Priorities

The Challenge

Problem: Adversary threats are outpacing policies and practices for engineering weapon systems; requires knowledgeable S&T and engineering workforce to provide dependably safe, secure, and resilient systems to operations at speed and scale

- **Advance policy and guidance to balance technology and program protection that enables rapid delivery of warfighter capability**
- **Strengthen System Security/Secure Cyber Resilient Engineering workforce through innovative education and training methods**
- **Advance Technology and Program Protection methods to ensure technological superiority**
- **Advance the practice of Trust and Assurance through Joint Federated Assurance Center**

Lead Policy :

- DoDI 5000.83, DoDI 5200.44, DoDD 5200.47E

Guidance:

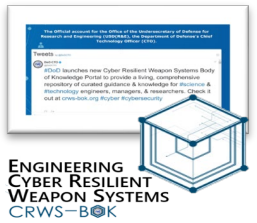
- Program Protection Planning
- Information Communications Technology Supply Chain
- Secure Software Supply Chain
- Software Assurance
- Controlled Technical Information
- Hardware Assurance
- Anti Tamper

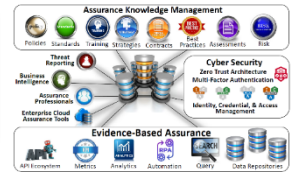
Standardization:

- Secure Cyber Resilient Engineering

Competency:

- System Security Engineering
- Secure Cyber Resilient Engineering





Joint Federated Assurance Center (JFAC)

Systems Security Mission: Foster Assured, Secure, Resilient Innovation, Missions, Systems and Components

Systems Security Directorate

Responsibilities:

Program Protection
Secure Cyber Resilient Engineering

- DoDI 5000.83, *Technology and Program Protection to Maintain Technological Advantage*
- Program Protection Plan
- Program Protection/cyber technical risk assessments
- Secure Cyber Resilient Engineering (SCRE) methods, and workforce
- SCRE Standards Area

- DFARS 252.204-7012 *Safeguarding Covered Defense Information and Cyber Incident Reporting*

Systems Security Policy, Guidance and Standards

ICT SCRM
Anti Tamper
Hardware Assurance

- DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks*
- DoDD 5200.47E, *Anti Tamper*
- Information Communications Technology Supply Chain Risk Management
- Critical program information identification
- Hardware Assurance

- DFARS 252.239-7018 *Supply Chain Risk*

System Security Engineering/Anti Tamper

ICT SCRM
Software Assurance
Secure Software Supply Chain

- Joint Federated Assurance Center Modernization
- Provides Federated Software Assurance tools, processes and expertise
- Partners with Military service leads to transition innovative Software Assurance Tools for use across the Department

Joint Federated Assurance Center/Software Assurance

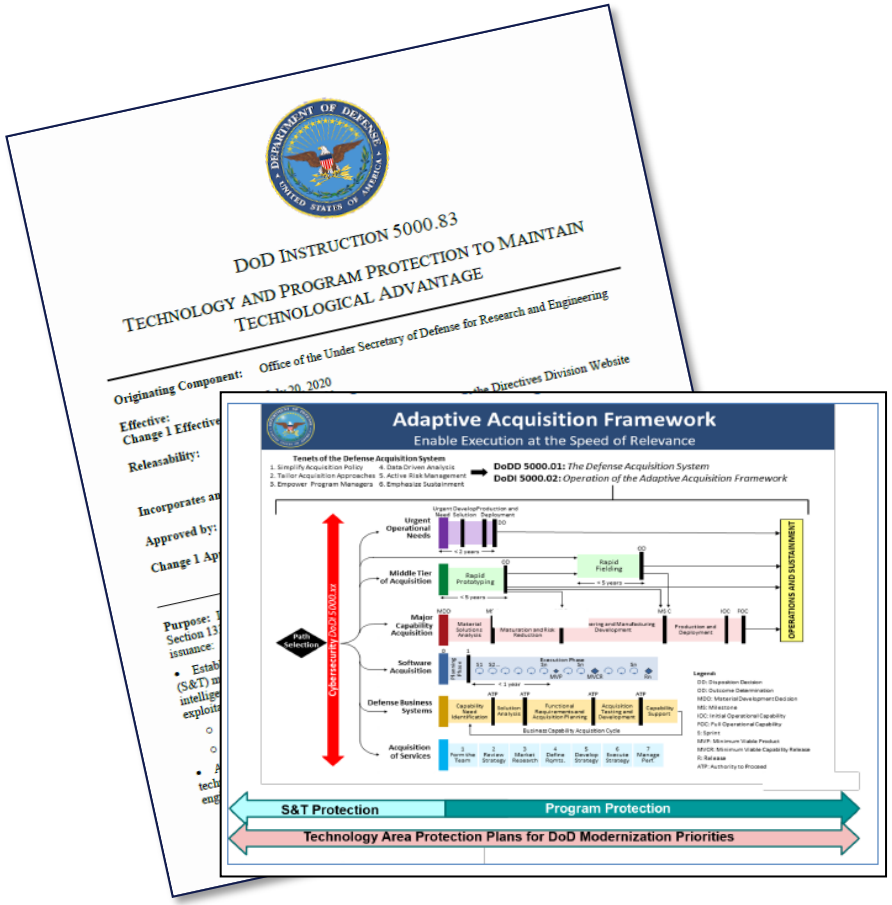
- Software Assurance Roadmap
- Innovative S&T software assurance mitigation and resilience needs
- Software Assurance mitigations
- Software Assurance mitigation approaches

- EO 14028 Improving the Nations' Cybersecurity-Secure Software Supply Chain and Software Bill of Materials

Software Assurance Technical Lead

MISSION: Foster Assured, Secure, Resilient Missions, Systems and Components

DoDI 5000.83: Technology and Program Protection



- **Establishes responsibilities and procedures for *S&T managers and engineers* to manage system security and cybersecurity technical risks to:**
  - DoD-sponsored research and technology
  - DoD warfighting capabilities
- **System security and cybersecurity technical risks include:**
  - Hardware, software, supply chain exploitation
  - Cyber, and cyberspace vulnerabilities
  - Reverse engineering, anti-tamper
  - Controlled technical information / data exfiltration
- **Employ systems security engineering and Secure Cyber Resilient Engineering methods**
- **Introduces S&T protection and Technology Area Protection Plans**
- **Points to Engineering and T&E issuance**
- **Aligns Program Protection Planning and Secure Cyber Resilient Engineering with acquisition pathways**

Establishes responsibilities for technology and program protection in support of the Adaptive Acquisition Framework; includes pre-acquisition protection activities

Technology and Program Protection to Maintain Technological Advantage

1. **GENERAL ISSUANCE INFORMATION**

2. **RESPONSIBILITIES**
   USD(R&E), USD(A&S), USD(I&S), DoD CIO, USD(P), DoD Component Heads

3. **PROCEDURES**

3.1. **TECHNOLOGY AND PROGRAM PROTECTION**
   a. Adversary impact on technology and programs
   b. Technologists and lead systems engineers responsibilities

3.2. **ACTIVITIES TO MITIGATE ADVERSARY THREATS TO TECHNOLOGY AND PROGRAMS**
   a. Safeguard Information
   b. Control DoD-sponsored research
   c. Design for security and cyber resiliency
   d. Protect the system against Cyberattacks from enabling and supporting systems
   e. Protect fielded systems
   f. Enhanced protections for critical programs and technologies

3.3 TECHNOLOGY AND PROGRAM PROTECTION MANAGEMENT
   a. Technology Area Protection Plan (TAPP)
   b. S&T Protection Plan
   c. Program Protection Plan (PPP)
   d. Independent Technical Risk Assessment (ITRA)
   e. System Engineering Plan (SEP)
   f. Test and Evaluation Master Plan (TEMP)
   g. Lifecycle Sustainment Plan

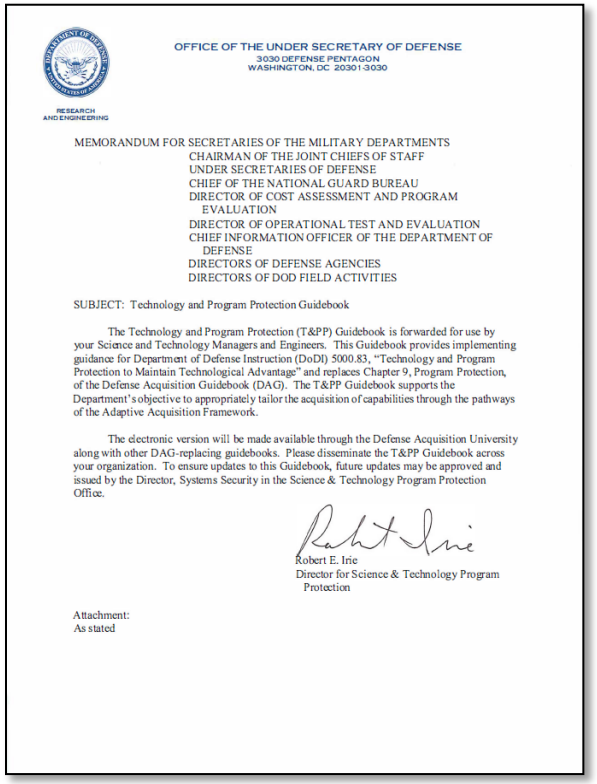
3.4 TAILORED PROGRAM PROTECTION FOR SELECTED ACQUISITION PATHWAYS
   a. Major capability acquisition
   b. Urgent operational needs
   c. Operation of the middle tier of acquisition
   d. Software acquisition

Prevent compromise or loss of critical technology transfer

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

Safeguard system and technical data from adversary collection and disruption

Technology and Program Protection Guidebook



OFFICE OF THE UNDER SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

RESEARCH AND ENGINEERING

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEF OF THE NATIONAL GUARD BUREAU
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES

SUBJECT: Technology and Program Protection Guidebook

The Technology and Program Protection (T&PP) Guidebook is forwarded for use by your Science and Technology Managers and Engineers. This Guidebook provides implementing guidance for Department of Defense Instruction (DoDI) 5000.83, "Technology and Program Protection to Maintain Technological Advantage" and replaces Chapter 9, Program Protection, of the Defense Acquisition Guidebook (DAG). The T&PP Guidebook supports the Department's objective to appropriately tailor the acquisition of capabilities through the pathways of the Adaptive Acquisition Framework.

The electronic version will be made available through the Defense Acquisition University along with other DAG-replacing guidebooks. Please disseminate the T&PP Guidebook across your organization. To ensure updates to this Guidebook, future updates may be approved and issued by the Director, Systems Security in the Science & Technology Program Protection Office.

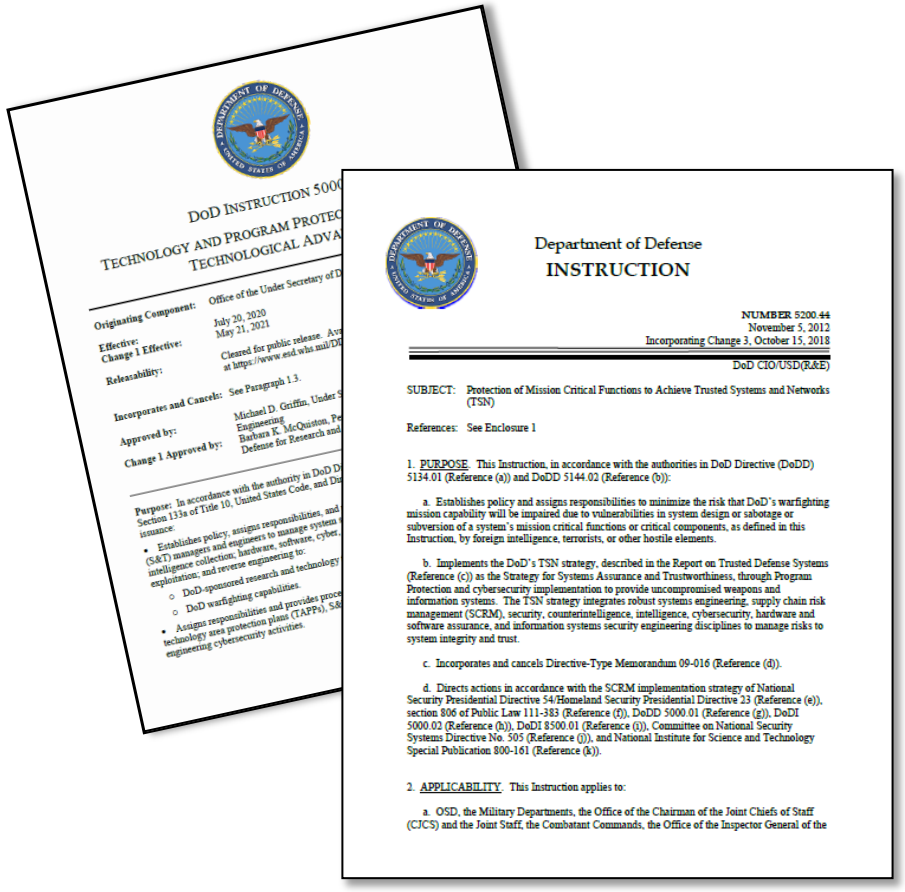
Robert E. Irie
Director for Science & Technology Program Protection

Attachment:
As stated

- **Provides implementing guidance for DoDI 5000.83, "Technology and Program Protection to Maintain Technological Advantage"**
  - Replaces Defense Acquisition Guidebook (DAG) Chapter 9, "Program Protection"
- **Incorporates technology protection activities for DoD-sponsored research and technology**
- **Emphasizes the S&T manager and engineering responsibilities for technology protection, program protection, and cyber**
- **Aligns S&T manager and engineering procedures with DoDI 5000.02, "Operation of the Adaptive Acquisition Framework"**

Supports the Department's objective to tailor acquisition of capabilities through the Adaptive Acquisition Framework pathways

DoDI 5200.44: Trusted Systems and Networks



Department of Defense
INSTRUCTION

NUMBER 5200.44
November 5, 2012
Incorporating Change 3, October 15, 2018
DoD CIO/USD(R&E)

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 5144.02 (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 cybersecurity implementation to provide uncompromised weapons and information systems. The TSN strategy integrates robust systems engineering, supply chain risk management (SCRM), security, counterintelligence, intelligence, cybersecurity, 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)), DoDD 5000.01 (Reference (g)), DoDI 5000.02 (Reference (h)), DoDI 8500.01 (Reference (i)), Committee on National Security Systems Directive No. 505 (Reference (j)), and National Institute for Science and Technology Special Publication 800-161 (Reference (k)).

2. APPLICABILITY. This Instruction applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the

- **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
  - Trusted supplier requirement for DoD-unique application-specific integrated circuits (ASICs)
- **Document Program's implementation and outcomes in Program Protection Plan and relevant cybersecurity plans, as appropriate**

Draft update incorporates procedures to implement information communication technology (ICT) exclusion authorities

Joint Federated Assurance Center

Mission: JFAC provides a federation of software and hardware assurance capabilities across the Department of Defense (DoD), supports implementation of DoDI 5200.44

Origin: Software Assurance FY13 NDAA Sec. 933, JFAC FY14 Sec. 937, 2015 DSD JFAC Policy Memo

System Application: DoD Weapon Systems, DoD Information Systems, and National Security Systems

Goals

- Stay Ahead of the Threat Landscape
- Migrate towards Holistic Assurance across the Life Cycle
- Maximize Discovery and Utilization of Federated Assurance Resources
- Mature Assurance Technologies and Deliver Capabilities at the Speed of Mission
- Provide Affordable and Scalable Assurance Solutions

Joint

Air Force | Army | Navy | OSD

Federated

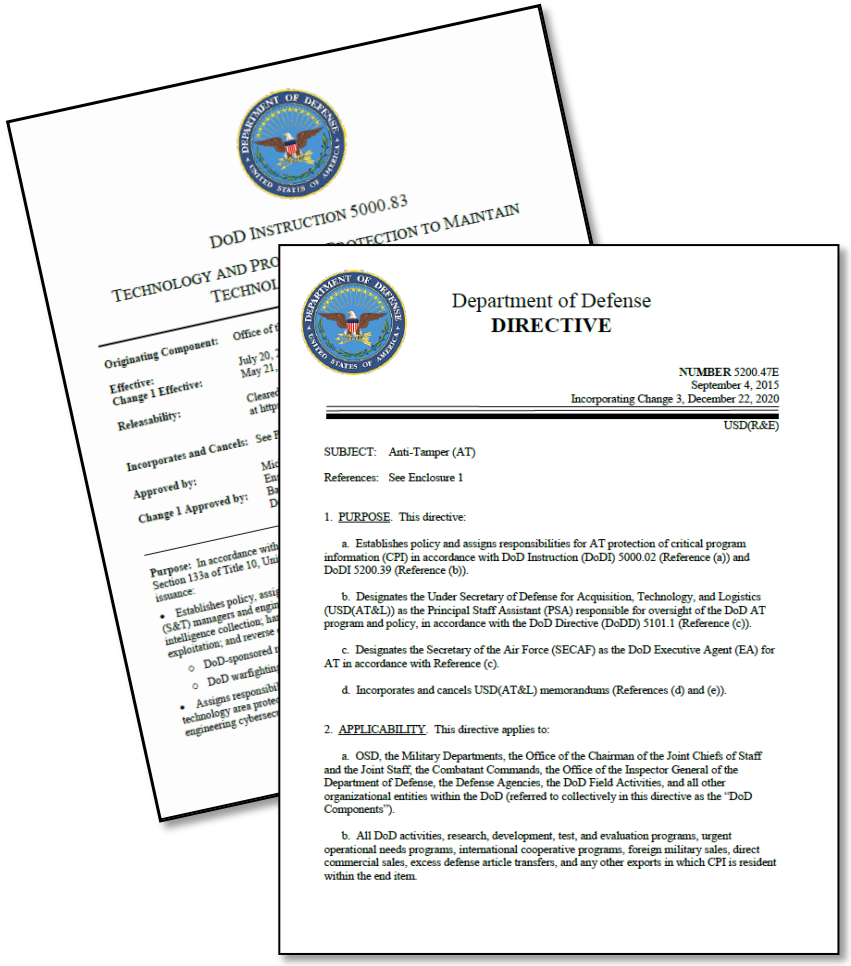
People / Organizations

Digital Infrastructure

Roadmap

JFAC Priorities	Current	Near Term	Mid Term	Long Term
Portal	Knowledge Management	Assurance Tool Catalog	Assurance Tool Market Place	
Assurance Technology	2017 Gap Assessment	S&T Assurance Projects	Assurance Investment Roadmap	
Assurance Assessment	Experts			Users
Assurance Licenses	Distributed COTS Tools	Assurance-as-a-Service	JFAC Sponsored Licenses Available via Market Place	

DoDD 5200.47E: Anti-Tamper



Department of Defense
DIRECTIVE

NUMBER 5200.47E
September 4, 2015
Incorporating Change 3, December 22, 2020
USD(R&E)

SUBJECT: Anti-Tamper (AT)

References: See Enclosure 1

1. PURPOSE. This directive:

a. Establishes policy and assigns responsibilities for AT protection of critical program information (CPI) in accordance with DoD Instruction (DoDI) 5000.02 (Reference (a)) and DoDI 5200.39 (Reference (b)).

b. Designates the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) as the Principal Staff Assistant (PSA) responsible for oversight of the DoD AT program and policy, in accordance with the DoD Directive (DoDD) 5101.1 (Reference (c)).

c. Designates the Secretary of the Air Force (SECAF) as the DoD Executive Agent (EA) for AT in accordance with Reference (c).

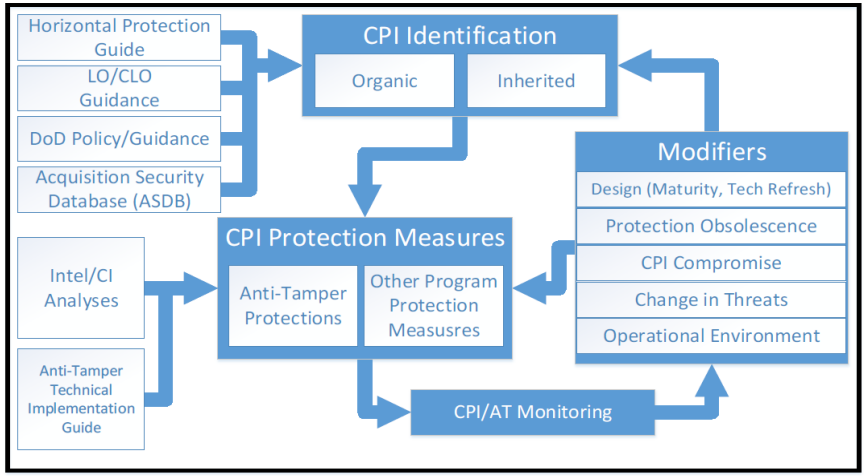
d. Incorporates and cancels USD(AT&L) memorandums (References (d) and (e)).

2. APPLICABILITY. This directive 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 (referred to collectively in this directive as the "DoD Components").

b. All DoD activities, research, development, test, and evaluation programs, urgent operational needs programs, international cooperative programs, foreign military sales, direct commercial sales, excess defense article transfers, and any other exports in which CPI is resident within the end item.

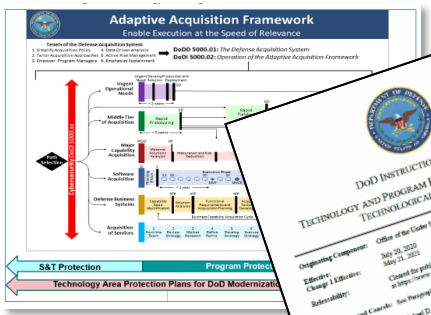
- **Establishes DoD Anti-Tamper (AT) Executive Agent**
- **Establishes responsibility for anti-tamper planning, implementation, and evaluations in alignment with guidance from the DoD Executive Agent for AT**

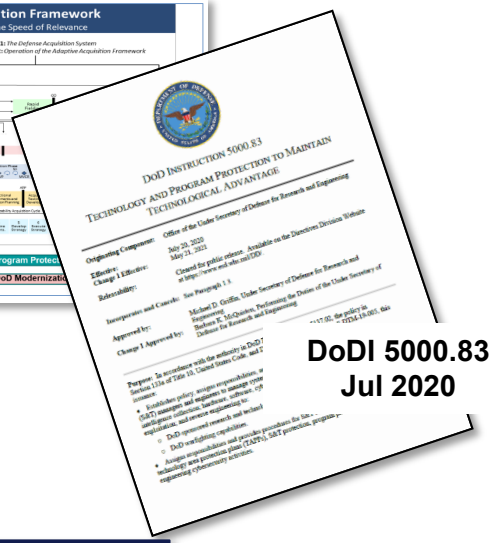


Established Critical Program Information Working Group across DoD stakeholders to identify efficiencies in the identification process

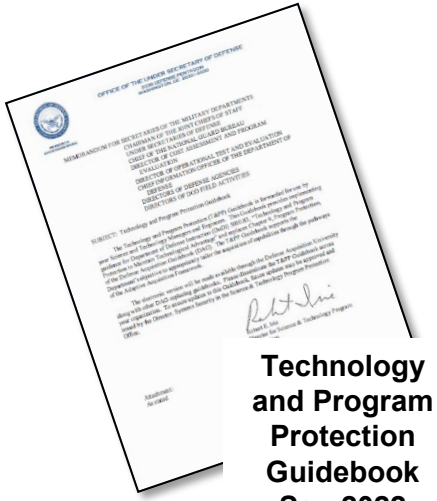
Draft update consolidates anti-tamper activities for the end item, to include identification of the end item

Alignment to the Adaptive Acquisition Framework

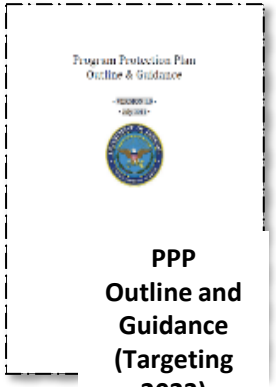




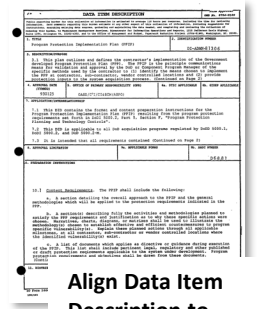
DoDI 5000.83 Jul 2020



Technology and Program Protection Guidebook Sep 2022

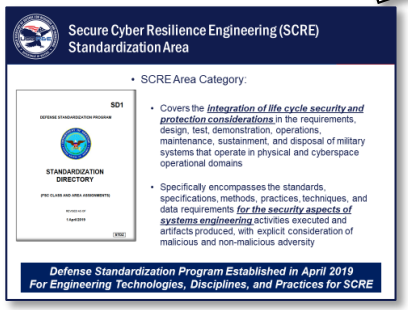


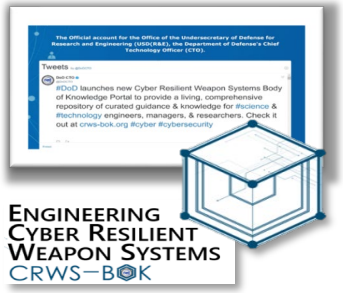
PPP Outline and Guidance (Targeting 2023)



Align Data Item Description to Updated Tables

- Fact of Life Policy Updates
- Acquisition Regulations updates
- Standardization
- Remove duplication
- Lessons Learned

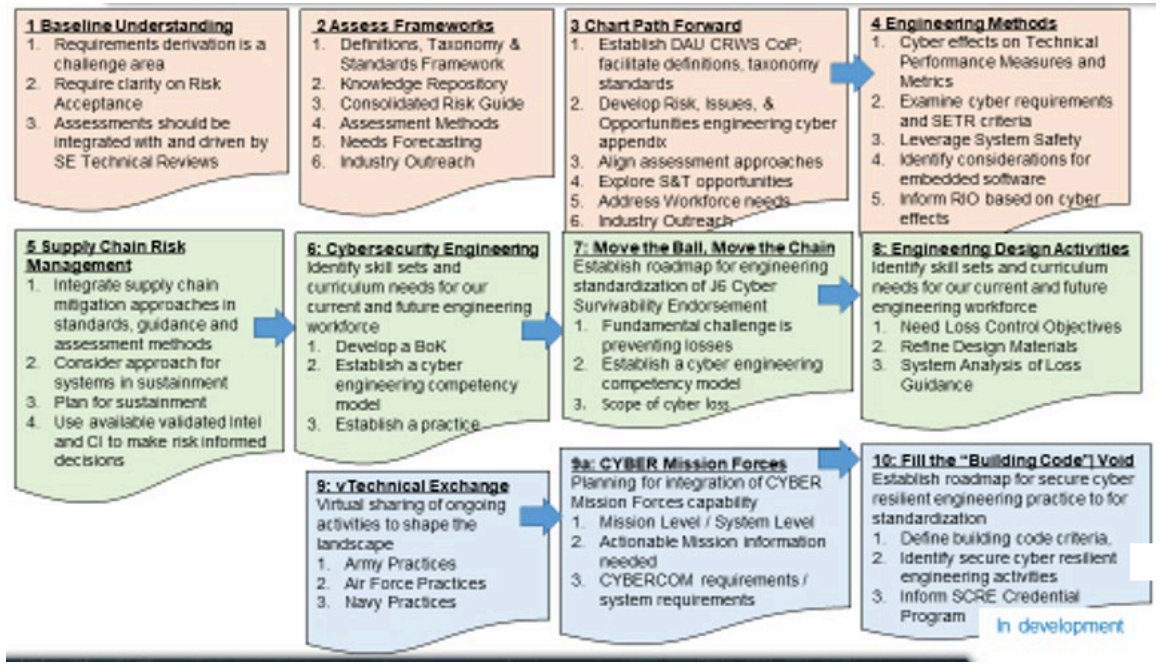




Support USD(R&E) Program Protection and Cyber Independent Technical Risk Assessments Assessments

2020 2021 2022 2023

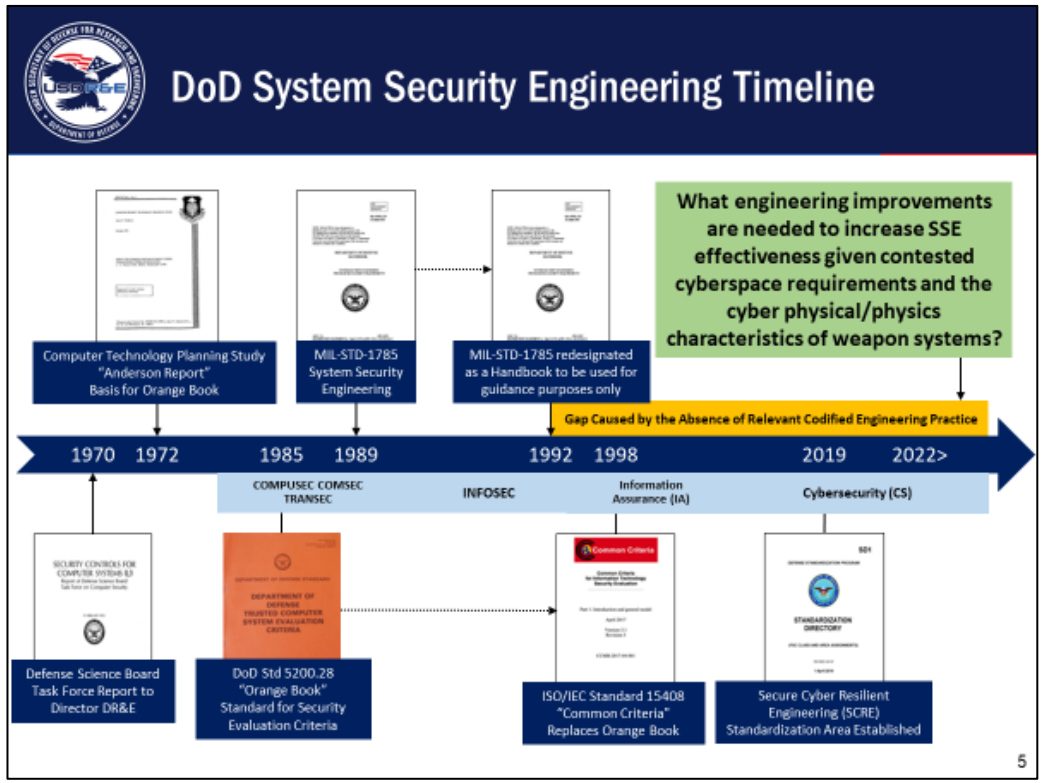
Engineering Cyber Resilient Weapon Systems Workshop Series

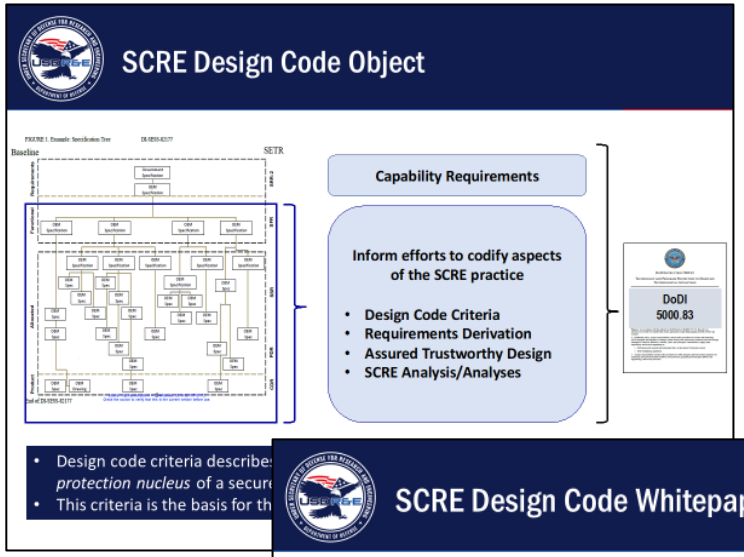


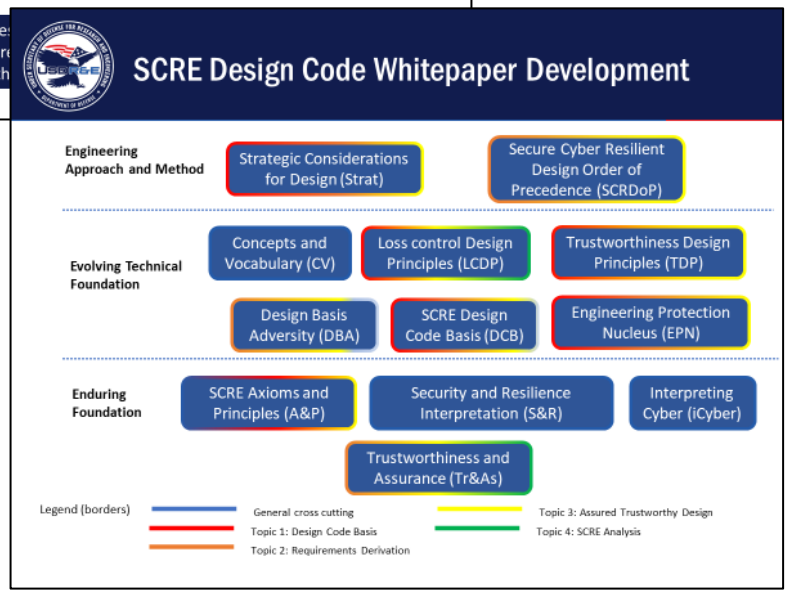
Collaboration Forum with Government, Industry, and Academia that builds upon each workshop to address challenges and lessons learned

- **March 2017:** Secure Cyber Resilient Engineering (SCRE) Standardization Area
  - Defense Standardization Program
- **August 2018:** CRWS Workshop Report: Preparing the Engineering Workforce for Cybersecurity Challenges
- **March 2019:** Draft SCRE Competency Model
- **November 2020:** DAU Approved to Establish the SCRE Credential Program
- **June 2021:** CRWS Book of Knowledge Deployment
- **August 2022:** 12 Secure Cyber Resilient Engineering Design Code White Papers

Secure Cyber Resilient Engineering Design Code







Advancing the Secure Cyber Resilient Engineering Practice and Standards

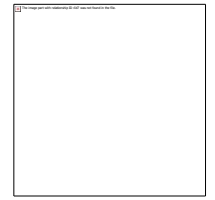
Workforce Competency

System Security Engineering

Secure Cyber Resilient Engineering

Defense Acquisition University

- Program Protection Credential Program
  - ACQ 160: Program Protection Planning Awareness
  - ENG 260: Program Protection for Practitioners
- CLE 022: Program Manager Introduction to Anti-Tamper



Defense Acquisition University

- Secure Cyber Resilient Engineering Credential Program
  - Under Development

Partnering with NDIA System Security Engineering Committee and DAU

- Controlled Technical Information Tabletop; findings and recommendations presented Feb. 2022
- Hardware Assurance Tabletop Tutorial initiative

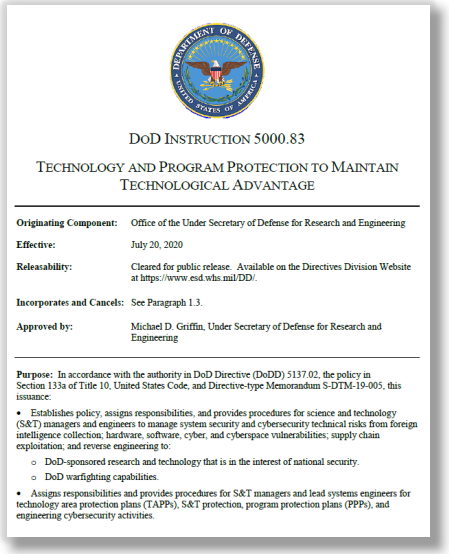
Summary

- **DoDI 5000.83 establishes roles and responsibilities for the S&T manager and engineering workforce**
- **Improve the efficiency and effectiveness of weapon systems engineering practice to deliver, and modernize, systems with the required capability in a secure manner under the presence of adverse conditions**
- **Increase consistency and repeatability of system security engineering and secure cyber resilient engineering methods and standards**
- **Improve the communication between government, industry, and operational stakeholders**

Customer-Focused: Outcome-Based

Backup

DoDI 5000.83: Technology and Program Protection to Maintain Technological Advantage



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.

Main Content

- **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 & Technology Protection Plans

- 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

DoD S&T (Budget Activities 6.1 - 6.4)

DoD RDT&E Programs (Budget Activities 6.4+)

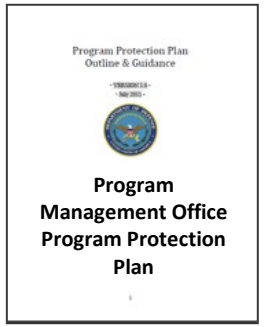
TAPP – Technology Area Protection Plan
PPP – Program Protection Plan

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

Delivering Assured, Secure, Resilient Systems

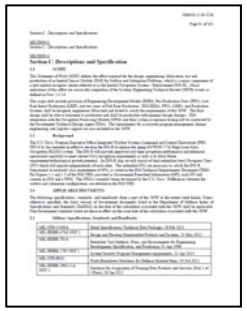
System Performance Specification
[Derived from JCIDS operational requirements]

Government Furnished Information



Program Management Office Program Protection Plan

Government Furnished Information

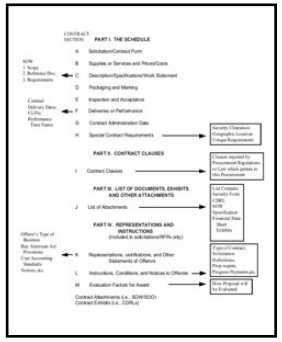


Section C Statement of Work

Contract Data Requirements List (CDRL): Contractor Program Protection Implementation Plan

Section I FAR/DFAR Contract Clauses

Consistent implementation will provide balanced and seamless protections



Solicitation/Contract

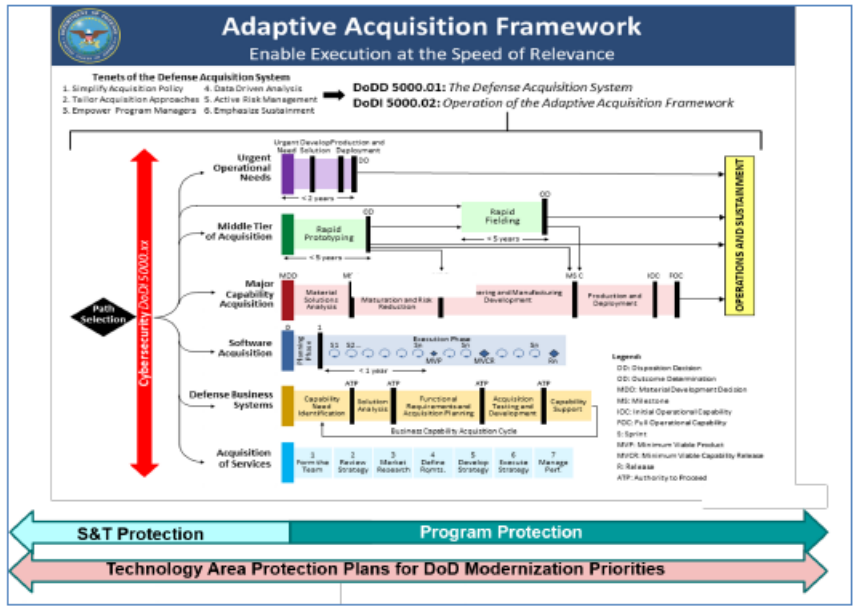
Increase consistency and repeatability of system assurance, system security, and cybersecurity methods and technologies

Improve expectations across Government, industry, academia and operational stakeholders

Adaptive Acquisition Framework Pathway Considerations

All program must consider program protection, however:

- Not all programs require PPPs
  - Business Systems & Service Contracts do not require PPPs
  - Only programs where the DAE is the milestone decision authority have to submit the PPP to USD(R&E) for approval
  - DoD Components determine approval levels for other PPPs
- Tailored based on the pathway and anticipated risks the program will encounter:



- All programs must follow pathway Statutory & Regulatory Requirements
- Should use ***streamlined***
  - Program Protection Trade-off Analyses
  - Information Analysis
  - Critical Program Information (CPI) Analysis
  - Trusted Systems & Network (TSN) Analysis
- Ensure operators are informed of operational risks when the system is fielded

Fostering Assured, Secure, Resilient Missions, Systems, and Components

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 (JFAC)

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, assured, secure and resilient systems