



Program Protection Plan Outline and Guidance

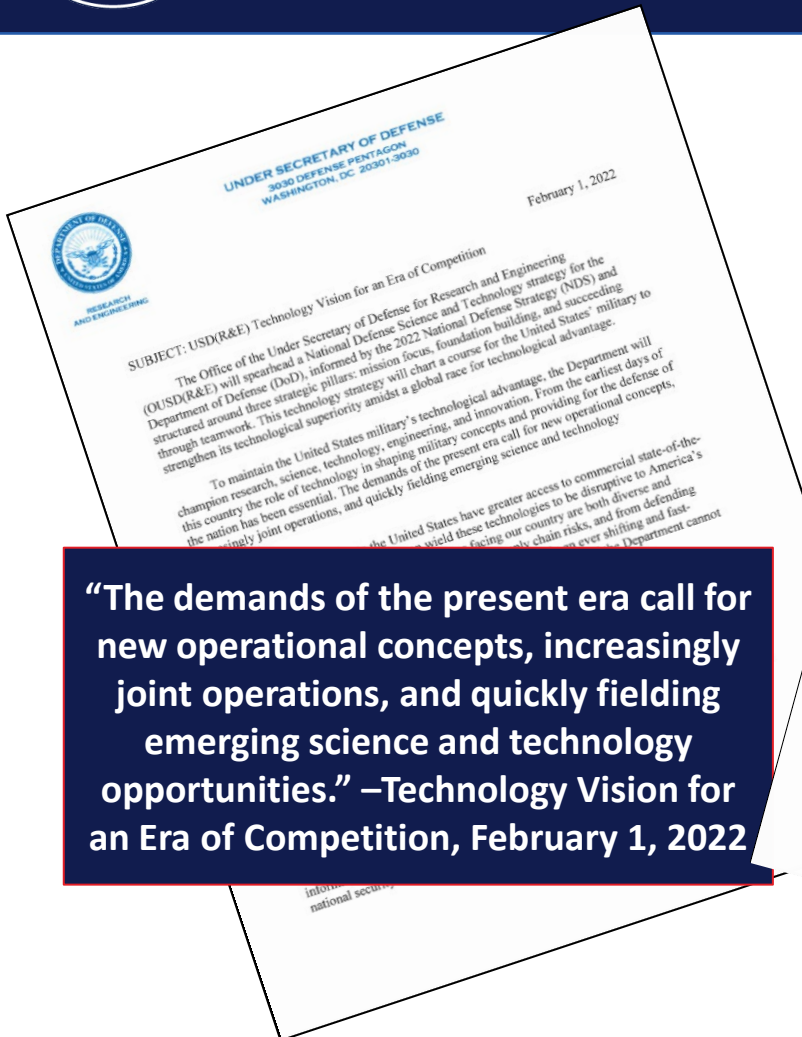
Update

16-19 October 2023

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



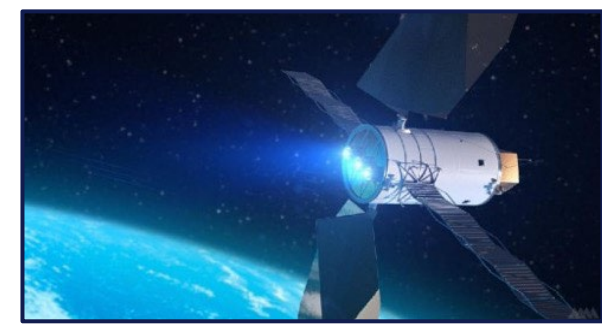
R&E Mission – Technology Vision in the Era of Competition



“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

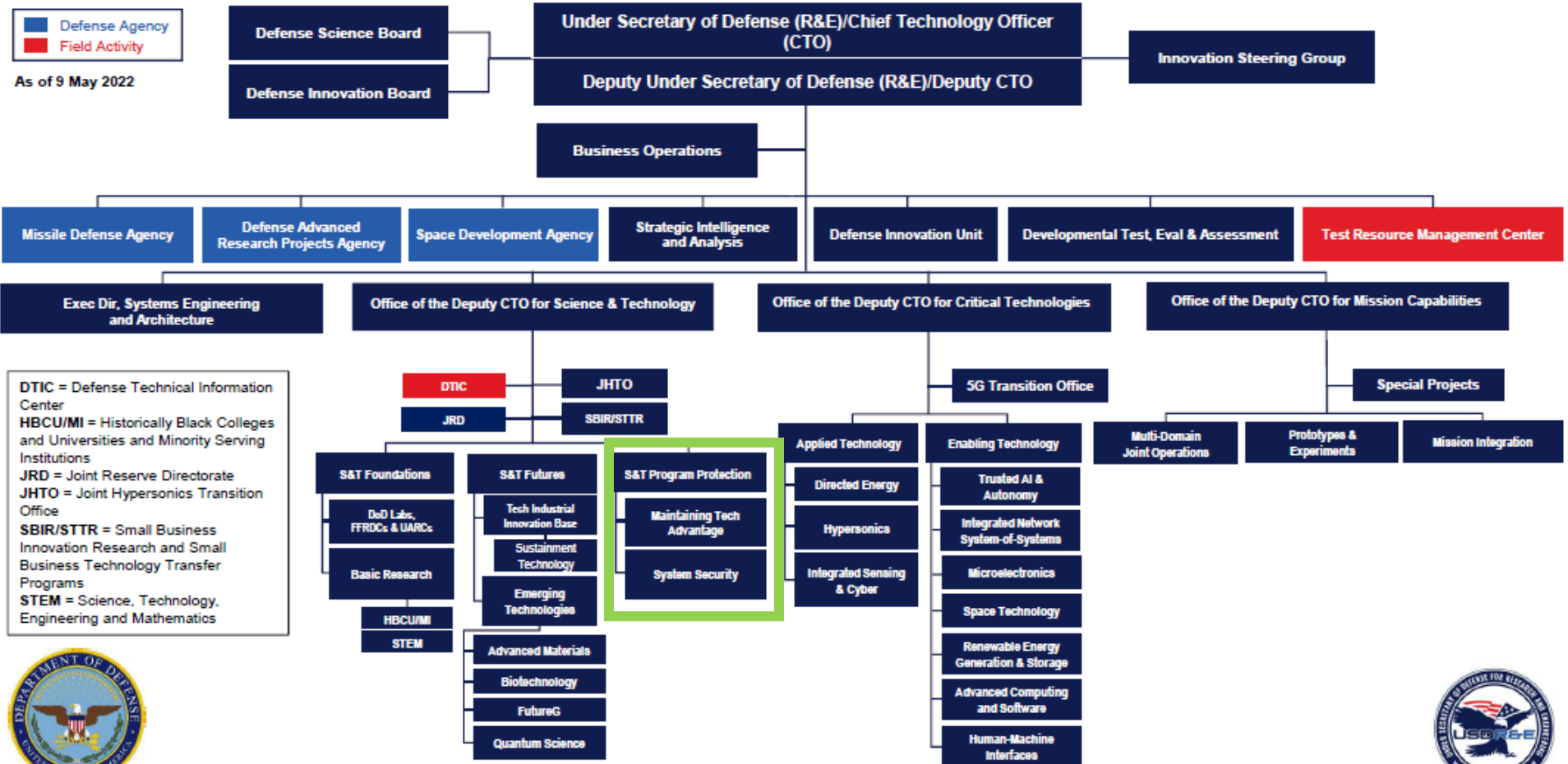
- Focus on the Joint Mission
- Create and field capabilities at speed and scale
- Ensure the foundations for research and development

Added NDTs





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



DTIC = Defense Technical Information Center
 HBCU/MI = Historically Black Colleges and Universities and Minority Serving Institutions
 JRD = Joint Reserve Directorate
 JHTO = Joint Hypersonics Transition Office
 SBIR/STTR = Small Business Innovation Research and Small Business Technology Transfer Programs
 STEM = Science, Technology, Engineering and Mathematics



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

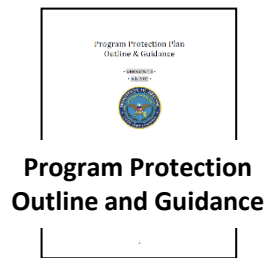
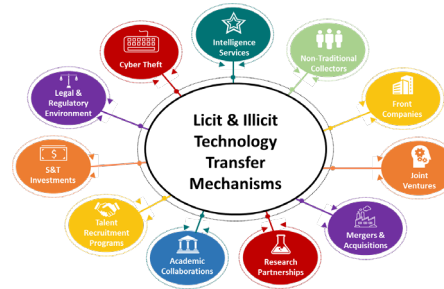


System Security Vision and Mission

Building Enduring Advantage

U.S. competitors increasingly hold at risk our defense ecosystem - the Department, the defense industrial base, and the landscape of private and academic enterprises that innovate and support the systems on which the Joint Force depends – NDS 2022

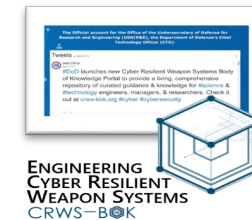
- **Adapt policy, guidance and standards to balance Technology and Program Protection that enables accelerated delivery of warfighter capability**
- **Cultivate the System Security, Secure Cyber Resilient Engineering workforce we need**
- **Strengthen Technology and Program Protection methods to ensure technological superiority**
- **Accelerate integration of data, software assurance, and microelectronics trust and assurance efforts through Joint Federated Assurance Center**



Program Protection Outline and Guidance



SCRE Standards Area
Standards, Specifications, Handbook, Data Item Descriptions and associated Guidance



ENGINEERING CYBER RESILIENT WEAPON SYSTEMS CRWS-BOOK



Joint Federated Assurance Center (JFAC)

Lead Policy :

DoDI 5000.83, DoDI 5200.44, DoDI 5200.NP, DoDD 5200.47E

Guidance:

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

Competency:

- System Security Engineering
- Secure Cyber Resilient Engineering

Engagements:

- CRWS Workshops
- NDIA SSE Committee

Provide the Department the Tools Needed to Build Cost Effective Enduring Advantage Through Resilient Assured, Secure, Innovation, Missions, Systems and Components



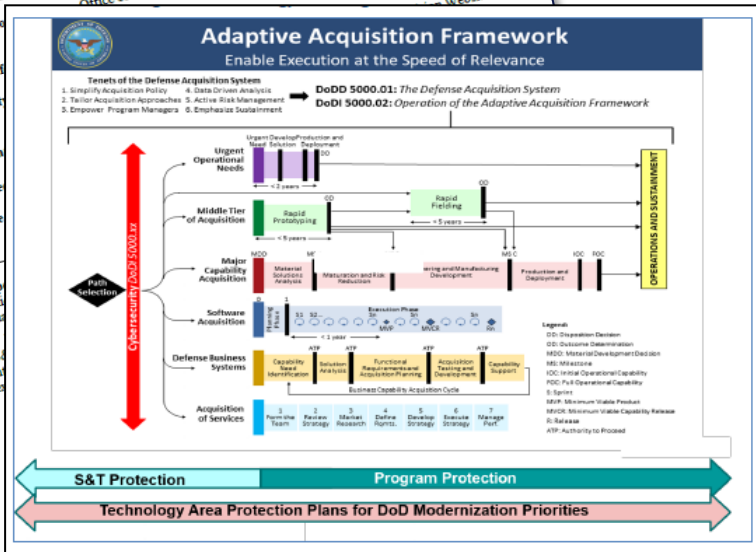
DoD Instruction (DoDI) 5000.83: Technology and Program Protection to Maintain Technological Advantage, Jul 2020



DoD INSTRUCTION 5000.83 TECHNOLOGY AND PROGRAM PROTECTION TO MAINTAIN TECHNOLOGICAL ADVANTAGE

Office of the Under Secretary of Defense for Research and Engineering

Originating Co
Effective: Change 1 Eff
Releasabili
Incorpora
Approve
Change
Purp
Sect
issu
(S
int

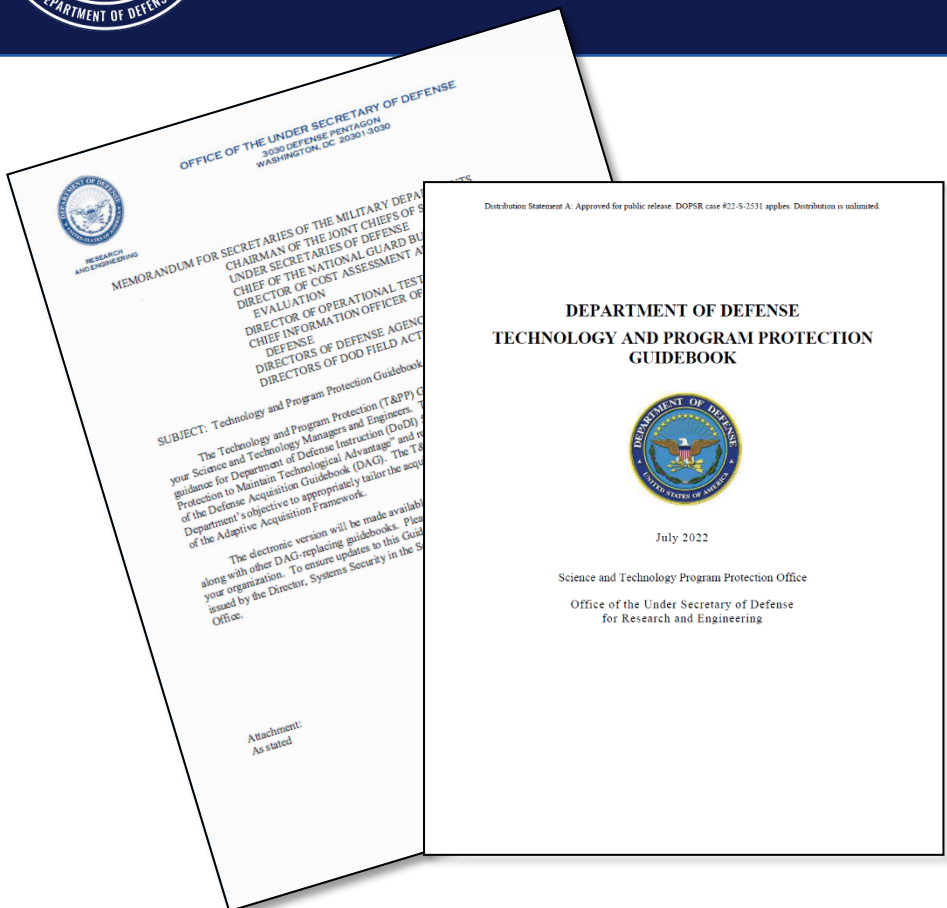


- Establishes responsibilities and procedures for S&T managers and engineers to manage systems security and cybersecurity technical risks to:
 - DoD-sponsored research and technology
 - DoD warfighting capabilities
- **Systems security and cybersecurity technical risks include:**
 - Hardware, software, supply chain exploitation
 - Cyber, and cyberspace vulnerabilities
 - Reverse engineering, anti-tamper
 - Controlled Technical Information / data exfiltration
- **Employs SSE and SCRE methods**
- **Introduces S&T protection and Technology Area Protection Plans (TAPPs)**
- **Points to Engineering and Test and Evaluation issuance**
- **Aligns Program Protection Planning and SCRE with acquisition pathways**

Establishes responsibilities for technology and program protection in support of the Adaptive Acquisition Framework; includes considerations to design for security and cyber resiliency



Technology and Program Protection Guidebook



- Provides implementing guidance for DoDI 5000.83, “Technology and Program Protection to Maintain Technological Advantage” includes
 - Applying marking and distribution statements on controlled technical information, Criticality Analysis, Software and Hardware Assurance, identification of critical program information for items that require anti tamper, and program protection planning
- 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”

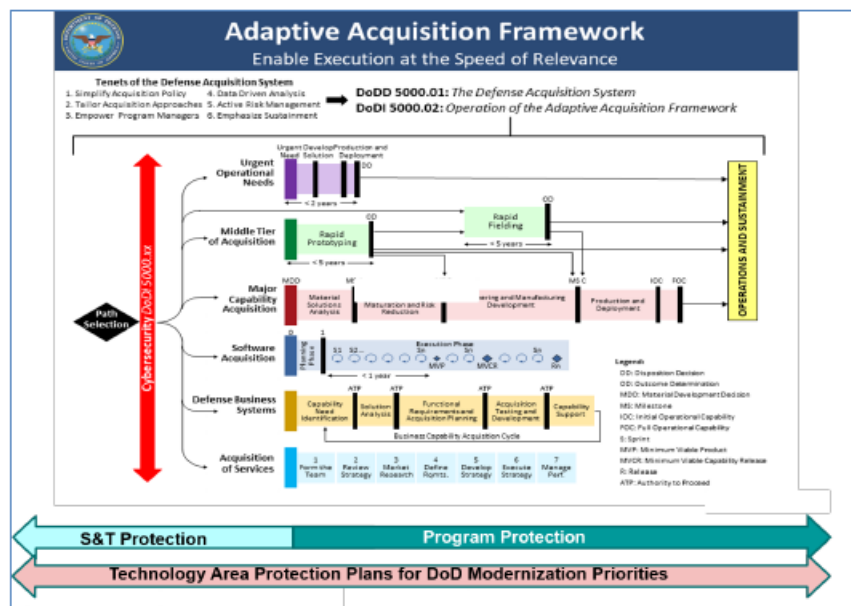
Supports the Department’s objective to tailor acquisition of capabilities through the Adaptive Acquisition Framework pathways



Adaptive Acquisition Framework Pathway Considerations

All program must consider program protection, however:

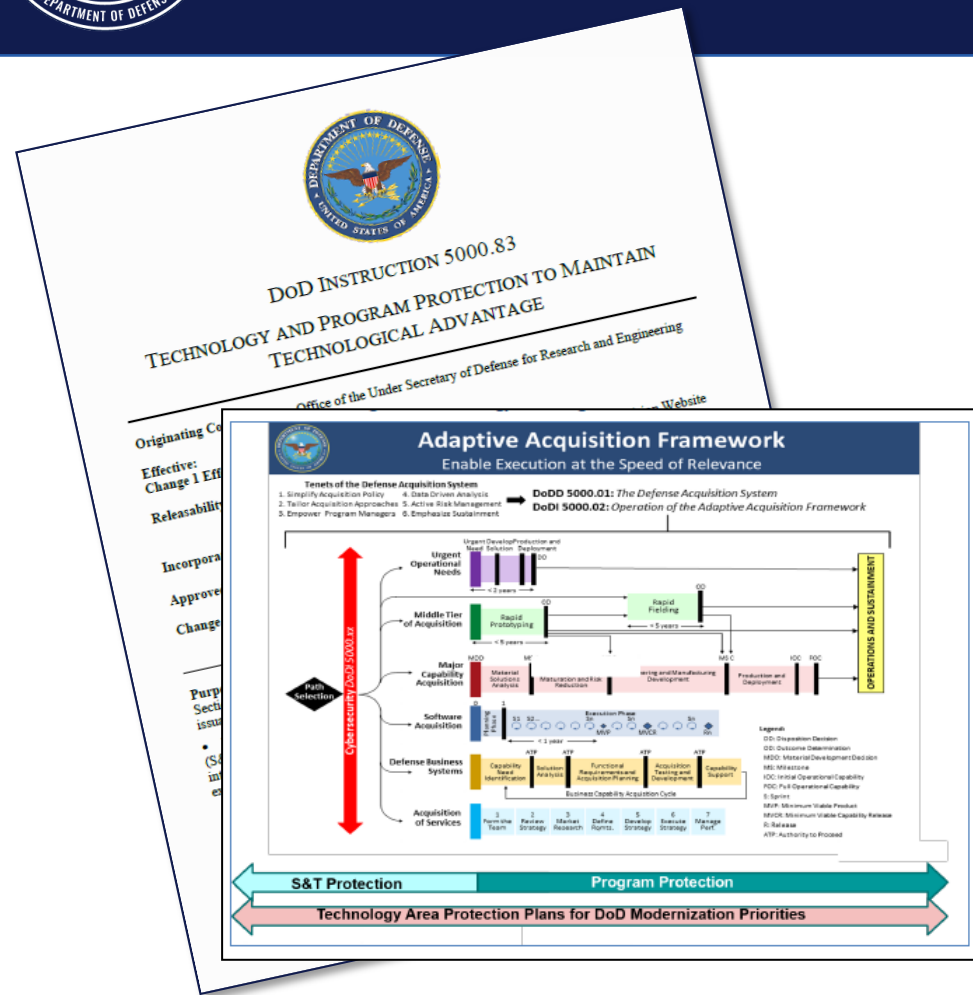
- Not all programs require PPPs
 - Business Systems & Service Contracts do not require PPPs
 - Only programs where the DAE is the milestone decision authority have to submit the PPP to USD(R&E) for approval
 - DoD Components determine approval levels for other PPPs
- Tailored based on the pathway and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



DoD Instruction (DoDI) 5000.83: Technology and Program Protection to Maintain Technological Advantage, Jul 2020



- Establishes responsibilities and procedures for S&T managers and engineers to manage systems security and cybersecurity technical risks to:
 - DoD-sponsored research and technology
 - DoD warfighting capabilities
- Systems security and cybersecurity technical risks include:
 - Hardware, software, supply chain exploitation
 - Cyber, and cyberspace vulnerabilities
 - Reverse engineering, anti-tamper
 - Controlled Technical Information / data exfiltration
- Employs SSE and SCRE methods
- Introduces S&T protection and Technology Area Protection Plans (TAPPs)
- Points to Engineering and Test and Evaluation issuance
- Aligns Program Protection Planning and SCRE with acquisition pathways

Establishes responsibilities for technology and program protection in support of the Adaptive Acquisition Framework; includes considerations to design for security and cyber resiliency



Program Protection Plan



Program Protection Plan Outline and Guidance as "Expected Business Practice"



PRINCIPAL DEPUTY UNDER SECRETARY OF DEFENSE
3015 DEFENSE PENTAGON
WASHINGTON, DC 20301-3015

JUL 18 2011

**MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
DIRECTORS OF THE DEFENSE AGENCIES**

SUBJECT: Document Streamlining - Program Protection Plan (PPP)

The September 14, 2010, Better Buying Power memorandum directed a review of the documentation required by Department of Defense Instruction (DoDI) 5000.02 in support of the acquisition process. This is the second in a series of document streamlining memoranda, following my April 20, 2011, direction on the streamlined Technology Development Strategy/Acquisition Strategy (TDS/AS) and Systems Engineering Plan outlines. I am directing the following actions for the PPP:

Document Streamlining: The PPP will be streamlined consistent with the attached annotated outline. The outline is designed to guide both program protection management and document preparation. It increases emphasis on early-phase planning activity and is specifically focused on information central to the purpose of the document. The new PPP reflects the integration of the Acquisition Information Assurance (IA) Strategy and recognizes Program Protection as the Department's holistic approach for delivering trusted systems.

PPP Review and Approval: Every acquisition program shall submit a PPP for Milestone Decision Authority review and approval at Milestone A and shall update the PPP at each subsequent milestone and the Full-Rate Production decision. While some programs may not have Critical Program Information, every program, including those with special access content, shall address mission-critical functions and components requiring risk management to protect warfighting capabilities. Per the TDS/AS outline described above, Program Protection information is no longer included in the TDS. The Acquisition IA Strategy shall continue to be reviewed and approved in accordance with DoDI 8500.1 and shall be included as an appendix to the PPP.

These actions constitute expected business practice and are effective immediately. The revised outline will be documented in the Defense Acquisition Guidebook and referenced in the next update to DoDI 5000.02. My point of contact is the Mr. Stephen Welby, Deputy Assistant Secretary of Defense for Systems Engineering, at 703-695-7417.

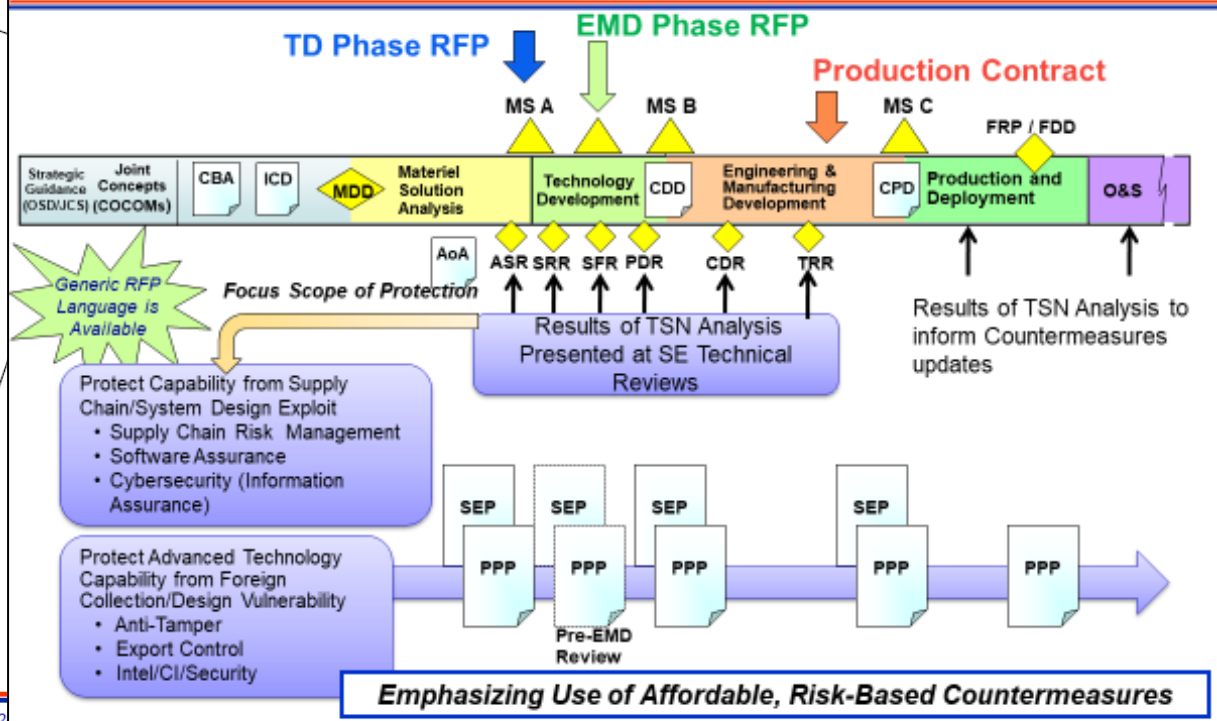
Frank Kendall
Frank Kendall
Deputy Assistant Secretary of Defense
Systems Engineering

**Program Protection Plan
Outline & Guidance**
• VERSION 1.0 •
• July 2011 •

<http://www.acq.osd.mil/se/pg/index.html#PPP>



PPP Development and Updates





Program Protection Plan Outline and Guidance Alignment



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

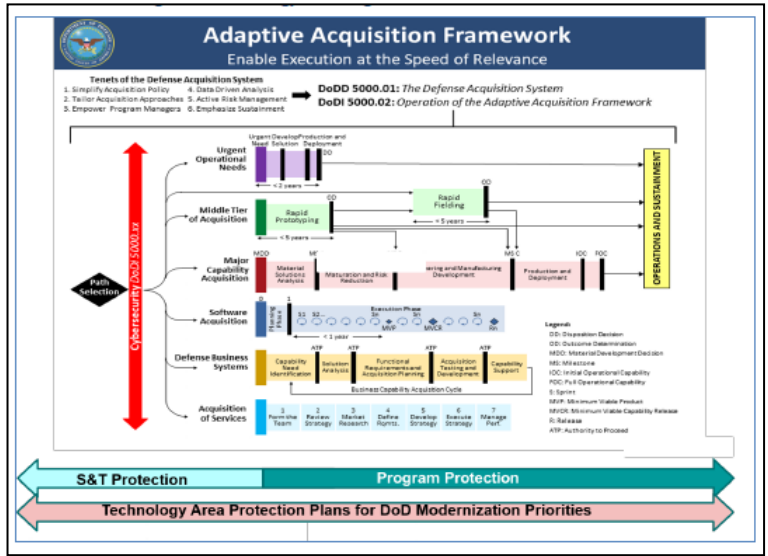
Updates to Defense Acquisition University (DAU) S&T managers and engineering education and training for technology and program protection will be informed by R&E-led Engineering Workforce Task Force

Collaboration with stakeholders is forthcoming

Distribution Statement A: Approved for public release. DOPSR case #20-S-1852 applies. Distribution is unlimited.

- **Align to DoDI 5000.83:**
 - Technology and Program Protection responsibilities for system and system security engineers
 - Engineers will tailor program protection based on the characteristics of the capability being acquired, including complexity, risk, and urgency to satisfy user requirements.

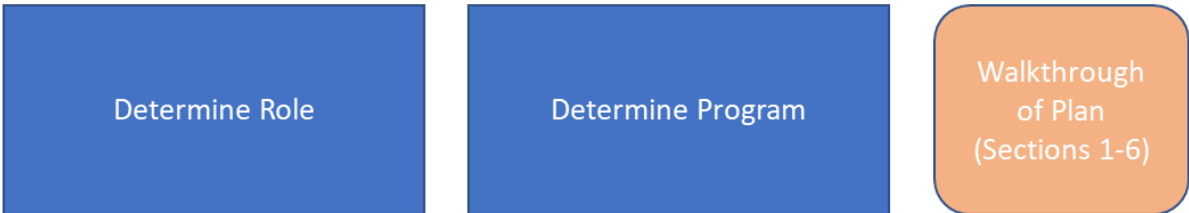
II. Create and field capabilities at speed and scale: Foster a more vibrant defense innovation ecosystem, accelerate the transition of new technology into the field, and communicate effectively inside and outside the Department.





Program Protection Plan Outline and Guidance Tabletop

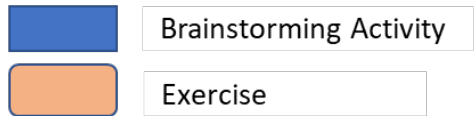
PLAN: Identify role and program to determine effectiveness of Sections 1-6



PROTECT: Define scenarios to exercise the implementation of protection methods and practices



RISK/ISSUES: Discuss existing risk process to determine feasibility of risk and issue documentation



- **Tabletops were face to face and supported virtual participation**

- Air Force
- Army
- Department of Navy
- Missile Defense Agency

- **Captured feedback throughout the process**

- **Adjudicated feedback to allow for tailoring to organizational needs**



Proposed Program Protection Plan Outline and Guidance Updates

- **Provides for tailoring to the Adaptive Acquisition Pathways**
- **Updated tables to capture fact of life changes**
- **Added table to capture Security Products and Services**
- **Added table to capture Federal Acquisition Regulation / Defense Federal Acquisition Regulation Supplement in contracts related to program**
- **Updated software assurance tables to include development frameworks, services, and reuse practices**

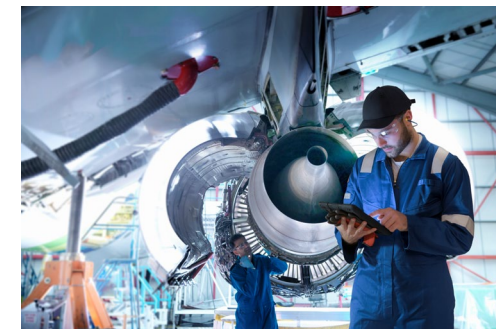
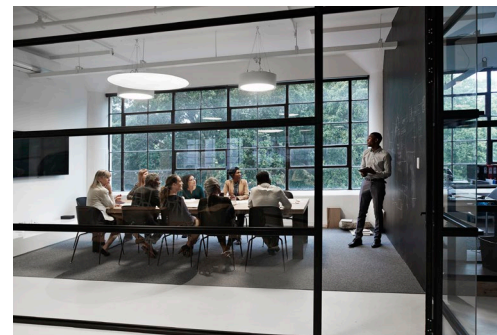


Next Steps

Program Protection Plan Outline & Guidance

DATA ITEM DESCRIPTION		Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information, to Washington Headquarters Service, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.			
1. TITLE	2. IDENTIFICATION NUMBER		
Program Protection Implementation Plan (PPIP)	DI-ADMN-81306		
3. DESCRIPTION/PURPOSE			
3.1 This plan outlines and defines the contractor's implementation of the Government developed Program Protection Plan (PPP). The PPPI is the principle communications means for validation and approval by the DoD or Component Program Manager of the specific methods used by the contractor to (1) identify the means chosen to implement the PFP at contractor, sub-contractor, vendor controlled locations and (2) provide protection inputs to the system acquisition process. (Continued on Page 2)			
4. APPROVAL DATE (FORMS)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE
930125	CASD/C1/CI4SCH (ASPO)		
7. APPLICATION/INTERRELATIONSHIP			
7.1 This DID contains the format and content preparation instructions for the Program Protection Implementation Plan (PPIP) resulting from the program protection requirements set forth in DoDI 5000.2, Part 5, Section F, "Program Protection Planning and Technology Controls".			
7.2 This DID is applicable to all DoD acquisition programs regulated by DoDD 5000.1, DoDI 5000.2, and DoD 5000.2-M.			
7.3 It is intended that all requirements contained (Continued on Page 2)			
8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMEC NUMBER	
		D6881	
10. PREPARATION INSTRUCTIONS			
10.1 <u>Content Requirements.</u> The PPPI shall include the following:			
a. A section detailing the overall approach to the PPPI and the general methodologies which will be applied to the protection requirements indicated in the PFP.			
b. A section(s) describing fully the activities and methodologies planned to satisfy the PFP requirements and justification as to why these specific actions were chosen. Narratives, charts, diagrams, or matrices shall be used to illustrate the methodology(s) chosen to establish effective and efficient countermeasures to program specific vulnerability(s). Explain these planned actions through all applicable milestones, at all contractor, sub-contractor or vendor controlled locations where the identified vulnerability(s) exist.			
c. A list of documents which applies as directive or guidance during execution of the PPPI. This list shall include pertinent legal, regulatory and other published or draft protection requirements applicable to the system under development. Program protection requirements and objectives shall be drawn from these documents. (Continued on Page 2)			
11. DISTRIBUTION STATEMENT			
DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited			
DD Form 1664, APR 89		Previous editions are obsolete.	
135/133		Page 1 of 2	

- Finalize Program Protection Plan Outline and Guidance update
- Develop / update Data Item Descriptions to align data needs to proposed tables
- Collaborate with NDIA SSE committee on proposed Data Item Descriptions



Microsoft 365 stock photos



Questions?