USD(R&E)

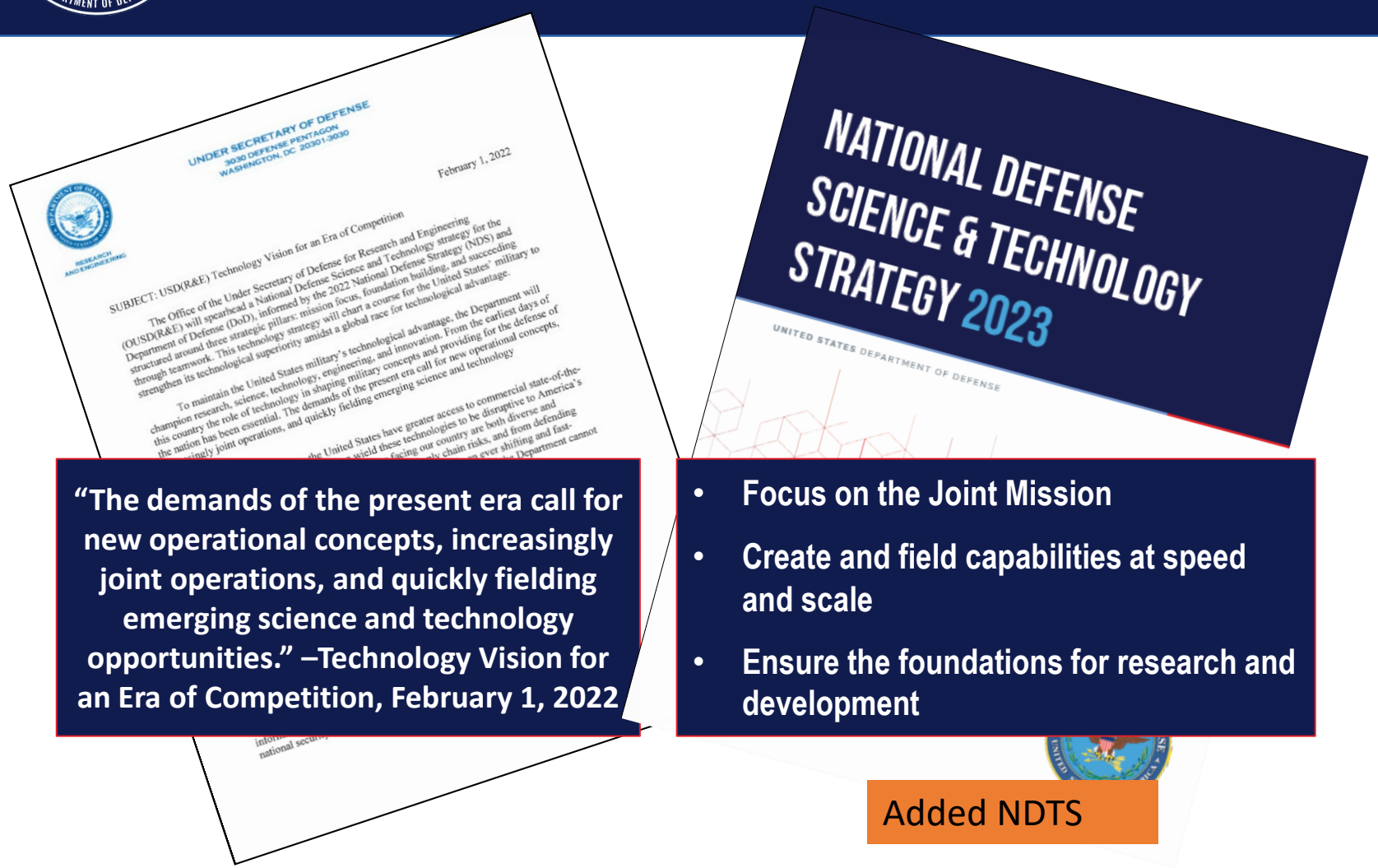
Program Protection Plan Outline and Guidance

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

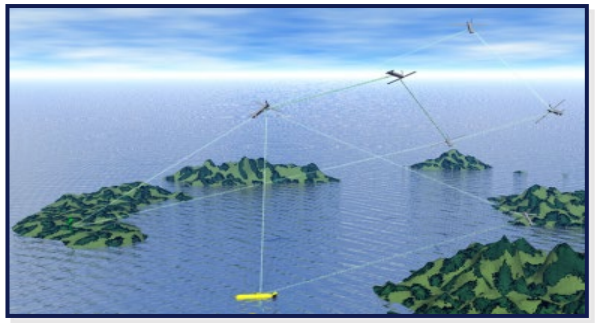
R&E Mission – Technology Vision in the Era of Competition

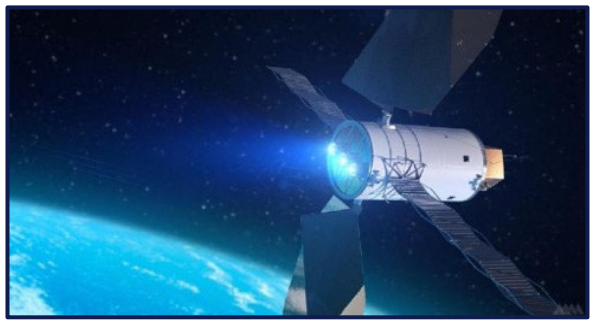


"The demands of the present era call for new operational concepts, increasingly joint operations, and quickly fielding emerging science and technology opportunities." –Technology Vision for an Era of Competition, February 1, 2022

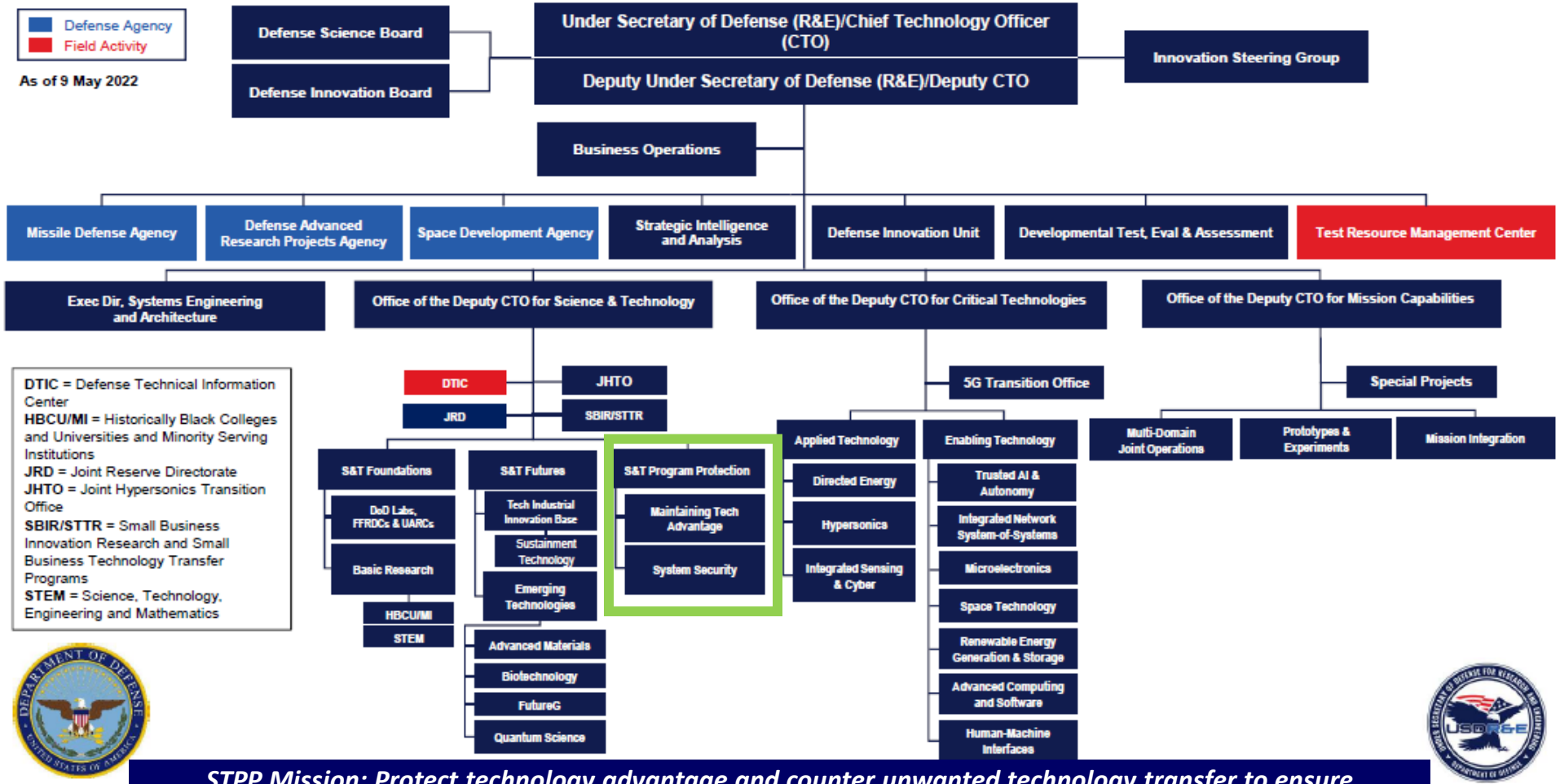
- **Focus on the Joint Mission**
- **Create and field capabilities at speed and scale**
- **Ensure the foundations for research and development**

Added NDTS





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



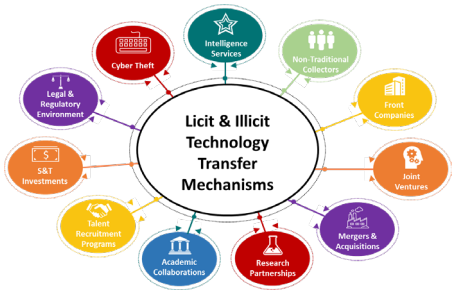
STPP Mission: Protect technology advantage and counter unwanted technology transfer to ensure warfighter dominance through assured, secure and resilient systems and a healthy viable national security innovation base

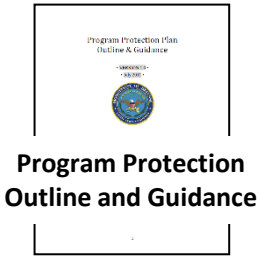
System Security Vision and Mission

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

Lead Policy :

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

Guidance:

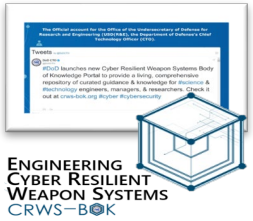
- Program Protection Planning
- Information Communications Technology Supply Chain
- Secure Software Supply Chain
- Controlled Technical Information
- Anti Tamper
- Hardware Assurance
- Microelectronics Assurance Framework
- Software Assurance

Competency:

- System Security Engineering
- Secure Cyber Resilient Engineering

Engagements:

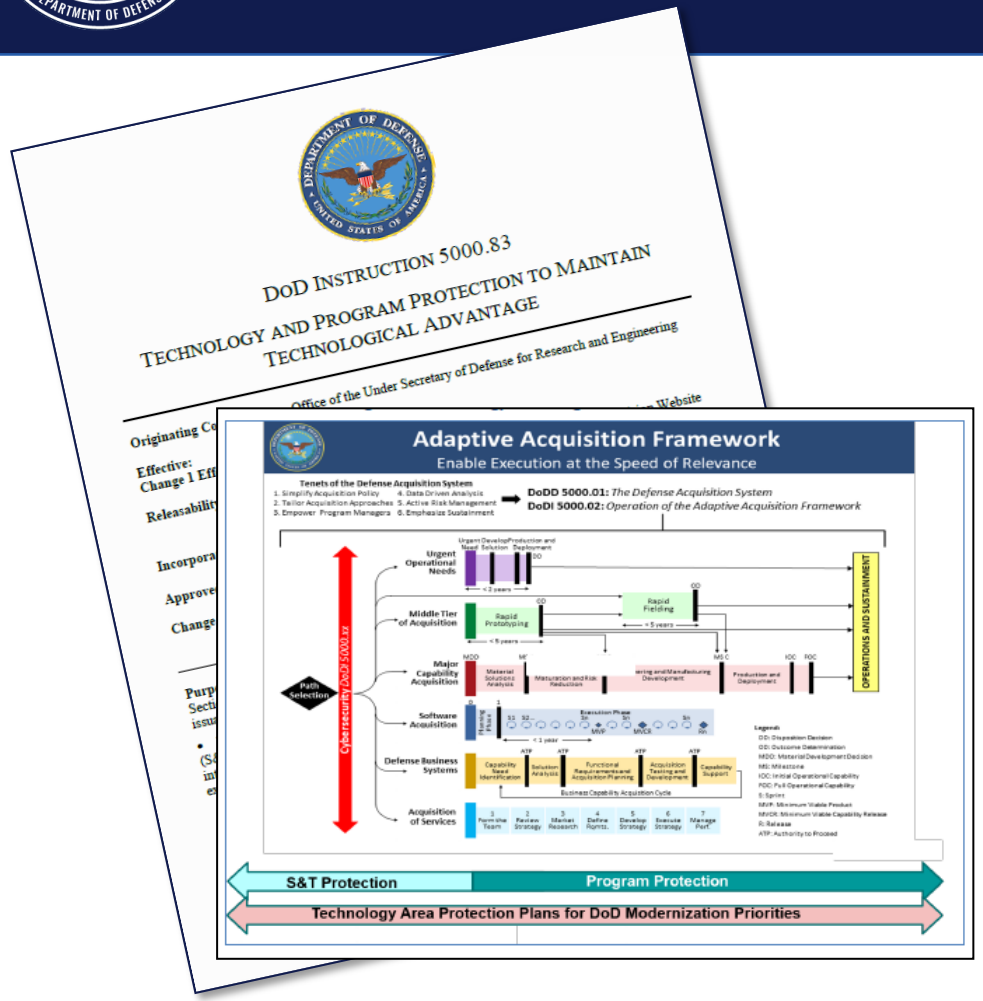
- CRWS Workshops
- NDIA SSE Committee



Joint Federated Assurance Center (JFAC)

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

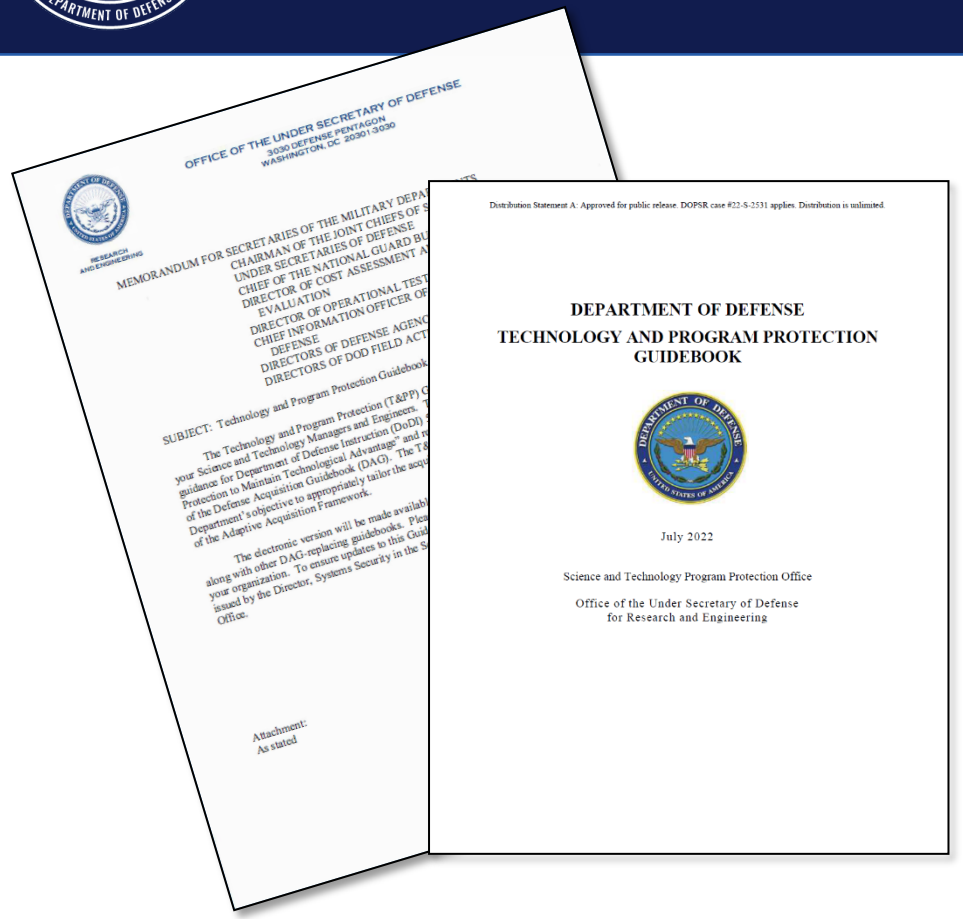
DoD Instruction (DoDI) 5000.83: Technology and Program Protection to Maintain Technological Advantage, Jul 2020



- **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



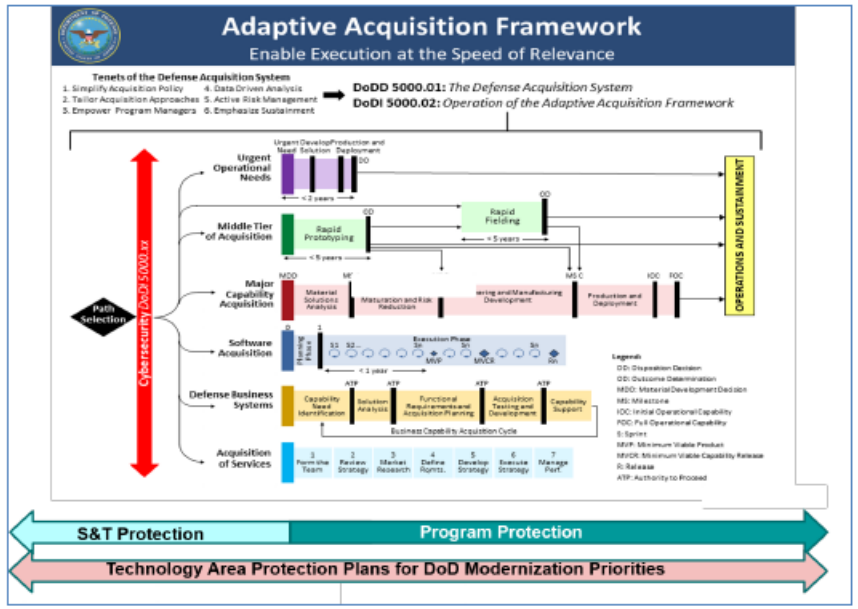
- **Provides implementing guidance for DoDI 5000.83, "Technology and Program Protection to Maintain Technological Advantage" includes**
  - Applying marking and distribution statements on controlled technical information, Criticality Analysis, Software and Hardware Assurance, identification of critical 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

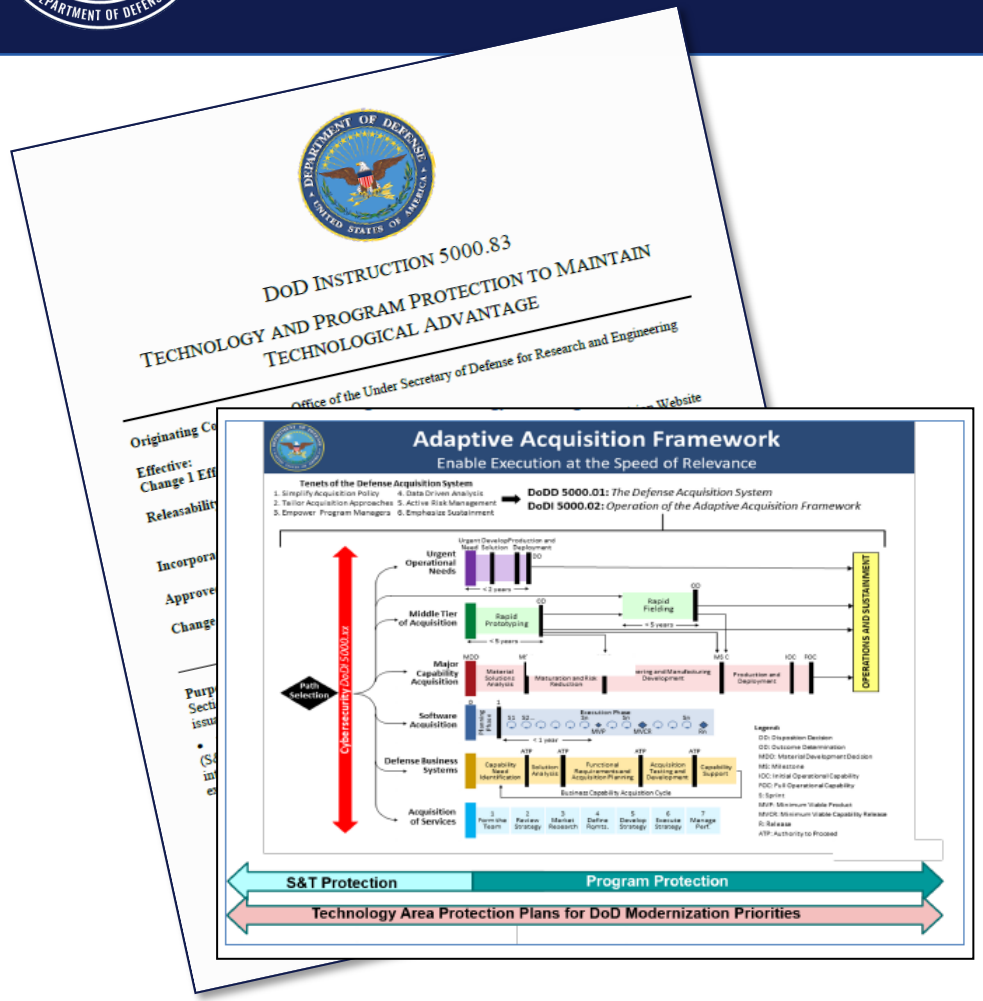
All program must consider program protection, however:

- 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

ACQUISITION, TECHNOLOGY AND LOGISTICS

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

cc:
All CAEs
DCMA
DCAA
DCMO
DASD(PSA)

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

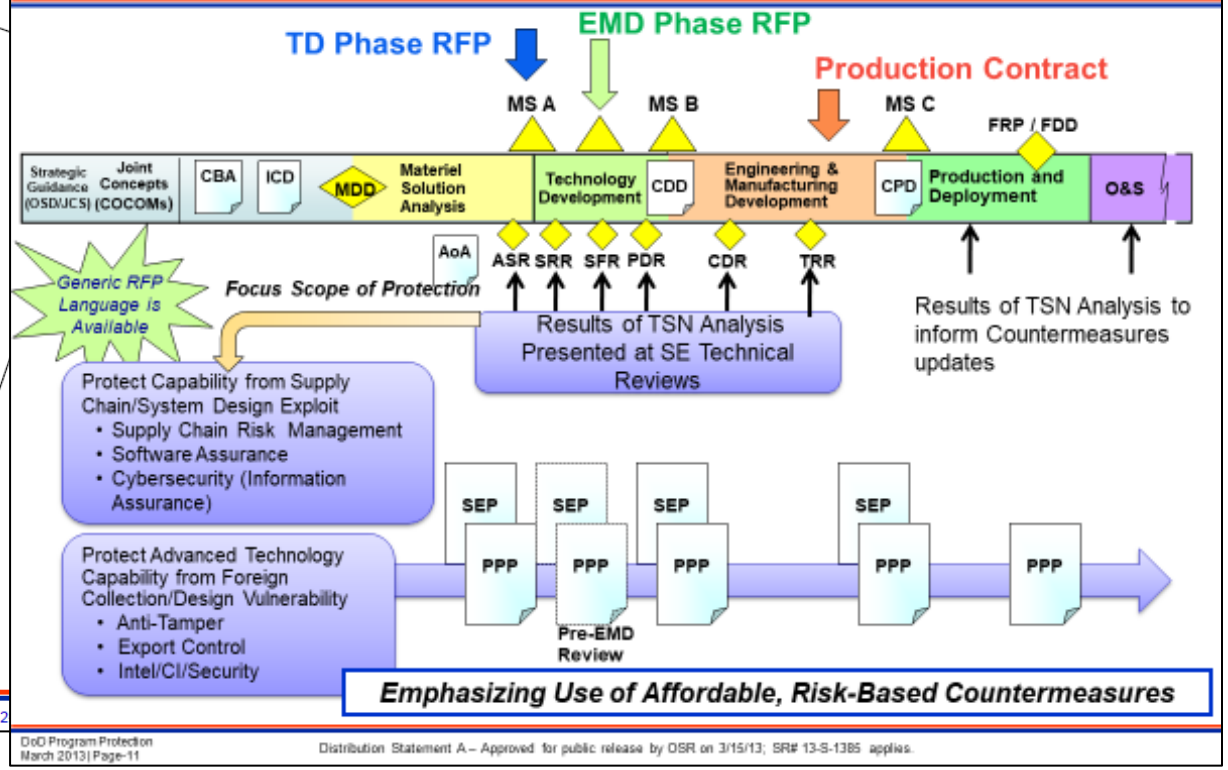
Deputy Assistant Secretary of Defense
Systems Engineering

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

US Policy and Process for Acquisition Security
V17h 4/11/12 Page 5

Distribution Statement A – Cleared for public release by OSR on 04/09/2012, SR Case #s 12-S-0754, 12-S-1188, 12-S-1193 and 12

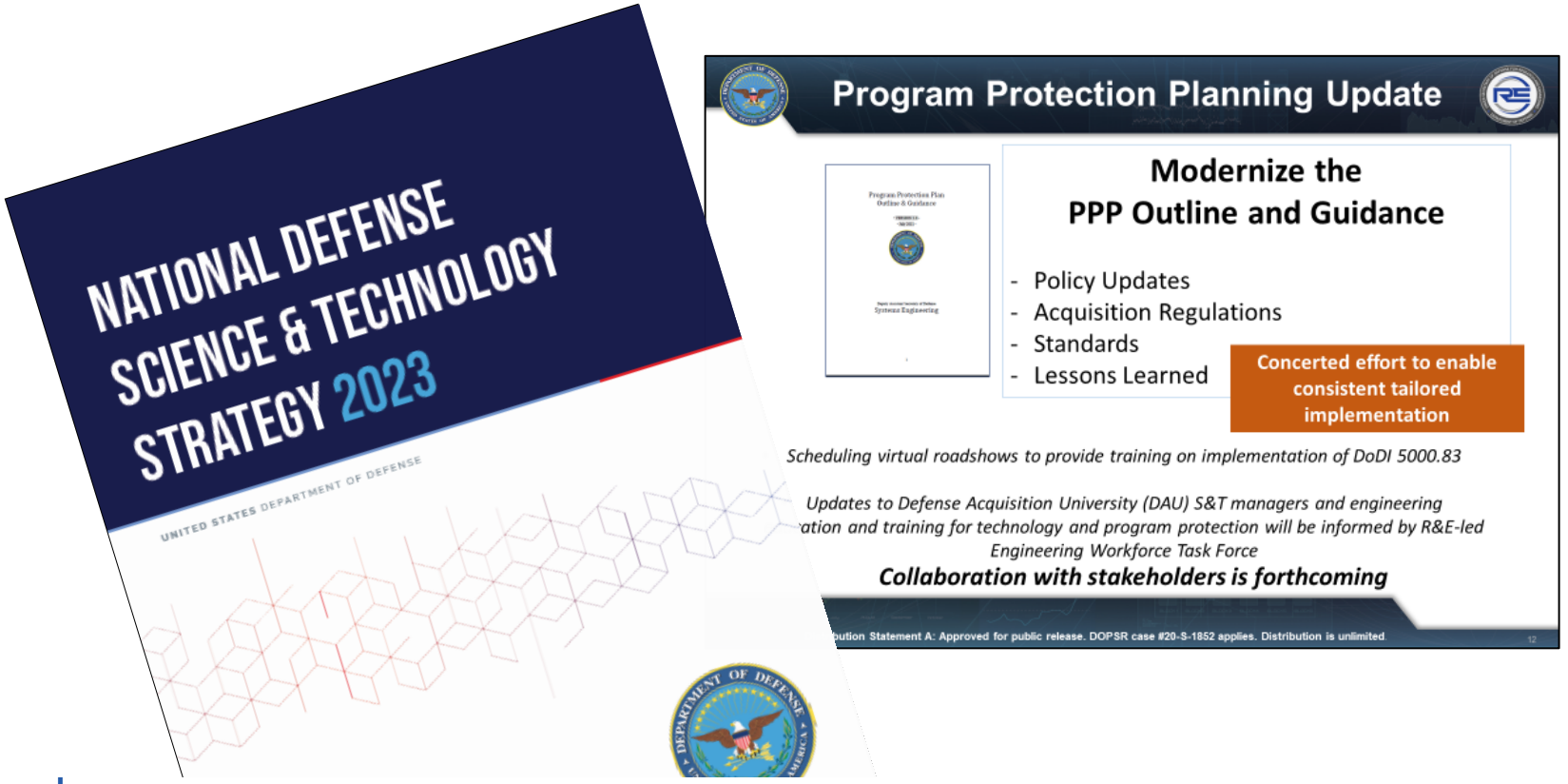
PPP Development and Updates



DoD Program Protection
March 2013 | Page-11

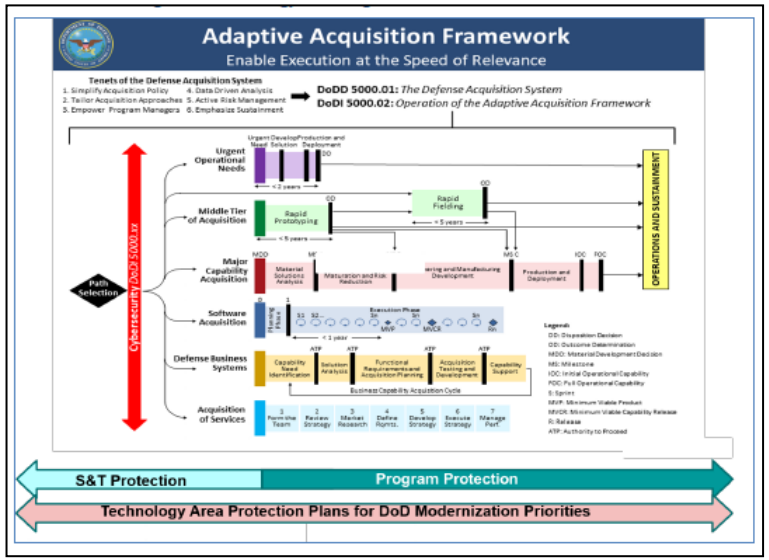
Distribution Statement A – Approved for public release by OSR on 3/15/13; SR# 13-S-1385 applies.

Program Protection Plan Outline and Guidance Alignment

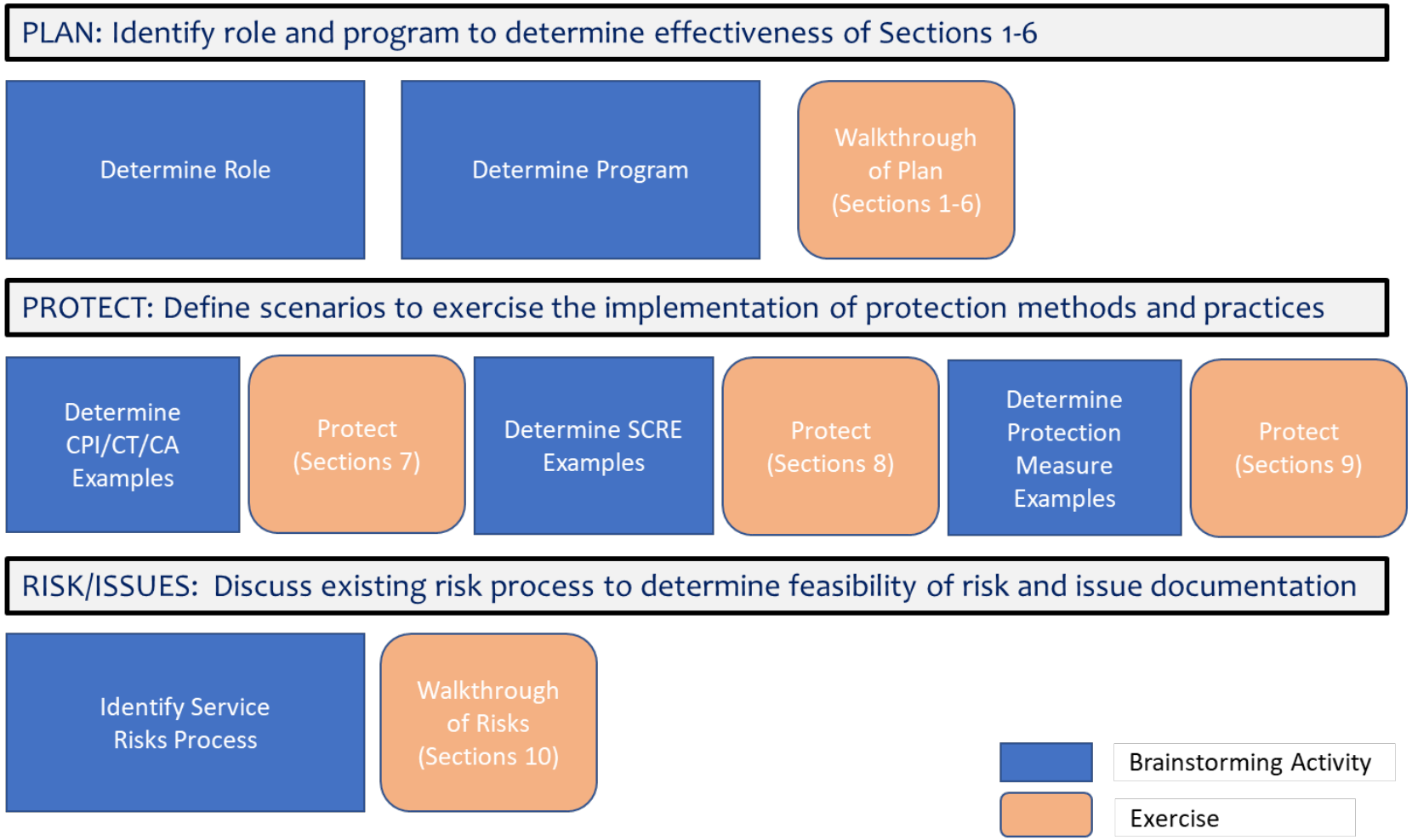


II. **Create and field capabilities at speed and scale:** Foster a more vibrant defense innovation ecosystem, accelerate the transition of new technology into the field, and communicate effectively inside and outside the Department.

- **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.



Program Protection Plan Outline and Guidance Tabletop

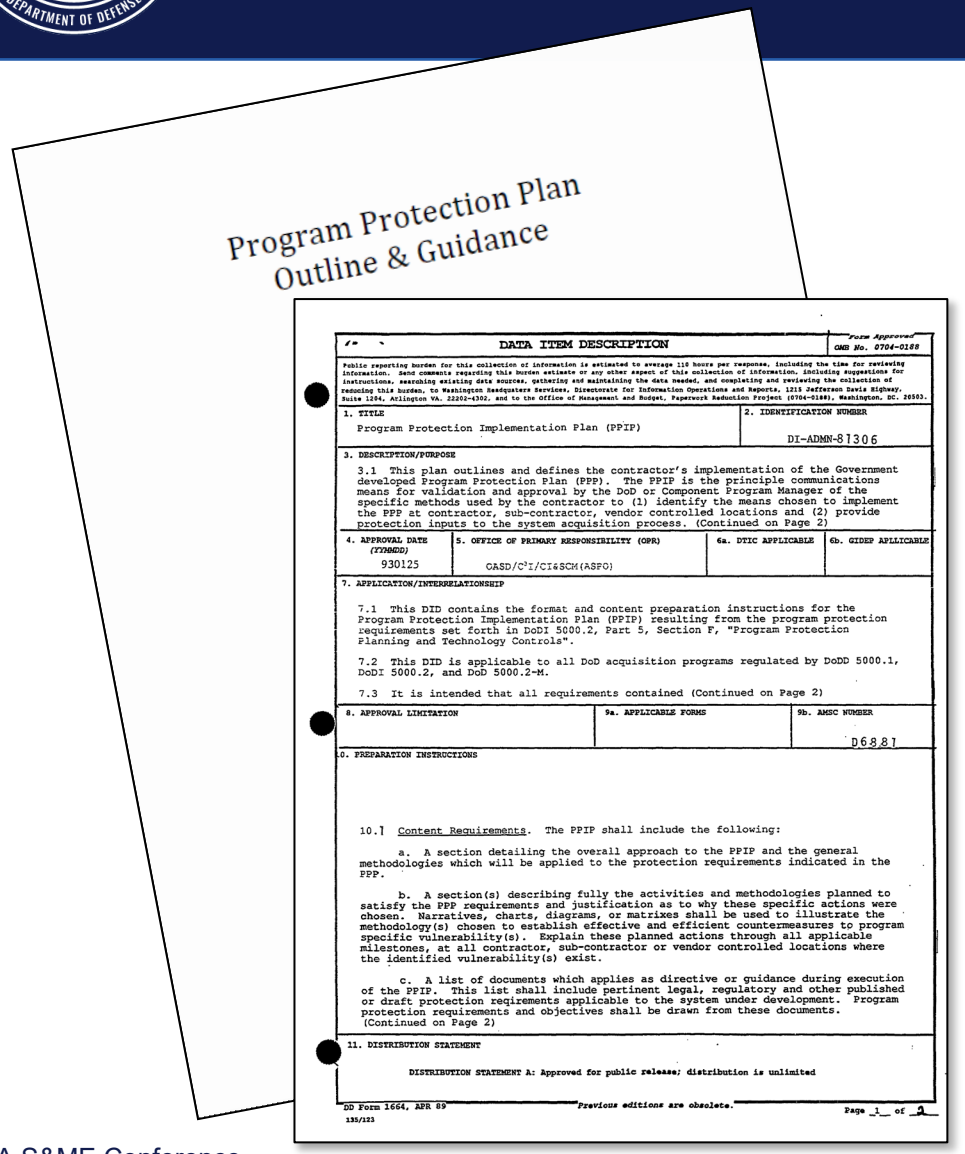


- **Tabletops were face to face and supported virtual participation**
  - **Air Force**
  - **Army**
  - **Department of Navy**
  - **Missile Defense Agency**
- **Captured feedback throughout the process**
- **Adjudicated feedback to allow for tailoring to organizational needs**

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



- **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?

14