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: **Change 1 Effective:**	July 20, 2020 May 21, 2021
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: **Change 1 Approved by:**	Michael D. Griffin, Under Secretary of Defense for Research and Engineering Barbara K. McQuiston, Performing the Duties of the 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.

TABLE OF CONTENTS

TABLES

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance applies to 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 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 issuance as the "DoD Components").

b. Nothing in this issuance alters or supersedes the existing authorities and policies of the Director of National Intelligence regarding the protection of sensitive compartmented information, as directed by Executive Order 12333 and other laws and regulations.

1.2. POLICY.

a. As a means to counter the threat from strategic competitor nations, the DoD will employ risk-based measures to protect systems and technologies from adversarial exploitation and compromise of U.S. military vulnerabilities and weaknesses in:

(1) Systems.

(2) Components.

(3) Software.

(4) Hardware.

(5) Supply chains.

b. Risk of adversarial exploitation and compromise of defense technology and programs will be managed, beginning with early S&T investment and continuing throughout the entire Defense Acquisition System (DAS) lifecycle, until disposal.

c. Programs will employ system security engineering methods and practices, including cybersecurity, cyber resilience, and cyber survivability in design, test, manufacture, and sustainment. Such methods and practices will ensure that systems function as intended, mitigating risks associated with known and exploitable vulnerabilities to provide a level of assurance commensurate with technology, program, system, and mission objectives.

d. TAPPs, S&T protection, and PPPs will be used to manage activities to protect and enable technology innovation for present and future warfighting capabilities and programs.

1.3. SUMMARY OF INCORPORATION AND CANCELLATION.

This issuance incorporates and cancels, or cancels portions of, DoD Instruction (DoDI) 5000.02T, as described in Tables 1 and 2. Upon publication of this issuance, DoDI 5000.02T will be administratively changed to remove the language canceled by this issuance.

Table 1. DoDI 5000.02T Change 8 Enclosure 3 Cancellation Actions

Enclosure 3 Paragraph	Action
11. Last sentence	Incorporates and Cancels
13. – 13.b.	Incorporates and Cancels

Table 2. DoDI 5000.02T Change 8 Enclosure 13 Cancellation Actions

Enclosure 13 Paragraph	Action
1.a.(1) – 1.a.(2)	Incorporates and Cancels
2.a. – 2.f	Incorporates and Cancels
3. – 3.a.(2)	Incorporates and Cancels
3. a. (7)	Incorporates and Cancels
3.b. – 3.b.(1)(c)	Incorporates and Cancels
3.b.(2) – 3.b.(2)(a).6.	Incorporates and Cancels
3.b.(3) – 3.b.(8)	Incorporates and Cancels
3.b.(10) – (12)	Incorporates and Cancels
3.b.(14)	Incorporates and Cancels
3.d. – 3.d.(2)	Incorporates and Cancels
3.e. – 3.e.(5)	Incorporates and Cancels
3.f.	Incorporates and Cancels
4.a. 4.b. 4.d.	Incorporates and Cancels
5. – 5.f.(7)	Cancels

1.4. SUMMARY OF CHANGE 1.

The changes to this issuance:

a. Correct the reference in Table 2 to the material in DoDI 5000.02T Change 8 being incorporated and cancelled by this issuance.

b. Correct minor administrative errors.

c. Update references for accuracy.

SECTION 2: RESPONSIBILITIES

2.1. UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING (USD(R&E)).

The USD(R&E):

a. Establishes and maintains S&T and program protection policy, guidance, education, and training to manage technical risk, including:

(1) Anti-tamper (AT).

(2) Hardware and software assurance.

(3) Supply chain risk management (SCRM).

(4) System assurance.

(5) Engineering secure cyber resilient systems.

b. Provides advice and makes recommendations to the Secretary of Defense and the Defense Acquisition Executive (DAE) on matters related to system security engineering, including:

(1) Cybersecurity, cyber resilience, and cyber survivability.

(2) Program protection risks to DoD-sponsored:

(a) Research.

(b) Technology.

(c) Programs.

(d) Systems.

(e) Capabilities.

c. Establishes and maintains TAPPs and associated policy, guidance, education, and training for designated modernization priorities as a means to achieve objectives for horizontal protection.

d. Is the PPP approval authority for Acquisition Category (ACAT) 1D Acquisition Programs.

e. Delegates approval authority to the Component acquisition executives or their designees for:

(1) ACAT 1B, ACAT 1C, ACAT II, and ACAT III PPPs for major capability programs.

(2) The PPPs for urgent, middle-tier programs (where the Component acquisition executive is the approval authority) and software acquisitions.

f. Establishes policy, guidance, education, and training for marking and disseminating controlled technical information (CTI), as described in DoDIs 5230.24 and 3200.12.

g. Establishes and maintains the DoD Joint Federated Assurance Center (JFAC) to develop and provide software and hardware assurance capabilities and expertise, as required by:

(1) DoD Policy Memorandum 15-001.

(2) Section 933 of Public Law 112-239.

(3) Section 937 of Public Law 113-66.

2.2. UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT (USD(A&S)).

As the DAE, the USD(A&S):

a. Includes technology area protection and program protection planning activities in the DAS to inform program and sustainment risk decisions.

b. Considers technology area protection and program protection planning activities when developing and implementing international acquisition and exportability features to ensure appropriate risk mitigation actions are taken with regard to acquisition systems.

c. In coordination with the USD(R&E), incorporates technology and program protection activities in Defense Acquisition University education and training.

2.3. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY.

In accordance with DoDD 5143.01, the Under Secretary of Defense for Intelligence and Security:

a. Oversees and directs the defense intelligence organizations in producing threat assessments to inform technical and procurement security risk mitigation activities.

b. Ensures the Defense Counterintelligence and Security Agency utilizes the Critical Program and Technology List to prioritize counterintelligence support and security activities in accordance with DoDD 5105.42.

c. Establishes policy, assigns responsibilities, and prescribes procedures for DoD controlled unclassified information (CUI).

d. Establishes and updates DoD policies for:

(1) Personnel security.

(2) Physical security.

(3) Industrial security.

(4) Classified information and CUI.

2.4. DOD CHIEF INFORMATION OFFICER.

In accordance with DoDD 5144.02, the DoD Chief Information Officer:

a. Provides guidance to the DoD Components on the risks that DoD systems are subjected to when connected to the DoD information enterprise, to the extent that the DoD information enterprise:

(1) Is effective.

(2) Can be relied upon in mitigating those risks.

b. Oversees DoD's Defense Industrial Base (DIB) Cybersecurity Program threat information sharing activities, in accordance with DoDI 5205.13.

2.5. UNDER SECRETARY OF DEFENSE FOR POLICY.

In accordance with DoDD 5111.01, the Under Secretary of Defense for Policy:

a. Provides technical analysis and technology transfer or export control input to TAPPs.

b. Uses TAPPs to inform international technology transfer activities and security countermeasures, including provisions for export controls.

c. Coordinates with the USD(R&E) to inform TAPPs of international technology transfer activities.

d. Develops policy and procedures for the Critical Program and Technology, in accordance with Section 1049 of Public Law 115-232.

2.6. DOD COMPONENT HEADS.

The DoD Component heads:

a. Establish policies, plans, and procedures for implementing this issuance.

b. Ensure:

(1) S&T, PPPs, and planning activities, when associated with critical technology or modernization priority areas, are consistent with applicable TAPPs and horizontal protection guidance.

(2) S&T and PPPs are approved by the appropriate authorities.

(3) Military Department counterintelligence organizations use the Critical Program and Technology List to support and prioritize counterintelligence activities in accordance with DoDI O-5240.24.

2.7. CHAIRMAN OF THE JOINT CHIEFS OF STAFF.

In addition to the responsibilities in Paragraph 2.6., the Chairman of the Joint Chiefs of Staff ensures that:

a. SCRM, export control, and AT requirements to achieve technology and program protection are:

(1) Included in capability requirements in the Joint Capability Integration and Development System (JCIDS).

(2) Addressed during capability development.

b. Counterintelligence and security support necessary to achieve technology and program protection throughout the lifecycle is identified in the JCIDS processes.

c. Information on foreign intelligence entity and cyber and supply chain threats are included in JCIDS capability requirements.

SECTION 3: PROCEDURES

3.1. GENERAL.

The overarching management policies governing the DAS are described in DoDD 5000.01 and DoDI 5000.02. The purpose of the DAS is to deliver effective and affordable solutions to the end user while enabling execution at the speed of relevance. To achieve that objective, the DoD employs an adaptive acquisition framework comprised of acquisition pathways (provided at https://aaf.dau.edu/aaf/), each tailored for the unique characteristics and risk profile of the capability being acquired. Technology area and program protection planning procedures will also be tailored for the:

a. Selected acquisition pathway.

b. Anticipated risks the program will encounter.

3.2. TECHNOLOGY AND PROGRAM PROTECTION.

a. Adversary Impact on Technology and Programs.

Mitigating adversary impact on technological advantage and employing system security engineering practices for program protection is a requirement for all DoD research, technology, and programs. Malicious activity by threat actors includes unauthorized activity to:

(1) Gain access to:

(a) DoD-sponsored research to erode competitive technical or economic advantage.

(b) DoD-advanced technology to erode U.S. technological superiority.

(c) Intellectual property, designs, or technical information to weaken U.S. technological and military advantage.

(2) Compromise or disrupt critical missions by gaining access to operational and classified information.

(3) Insert malicious, or exploit existing, vulnerabilities in hardware or software to disrupt or degrade system performance.

(4) Subvert or compromise DoD:

(a) Technology;

(b) Systems;

(c) Enabling systems; or

(d) Support systems.

b. S&T Managers and Lead Systems Engineers Responsibilities.

DoD technology, programs, systems, networks, supporting contract facilities, and activities are at risk of attacks by state and non-state threat actors. S&T managers and lead systems engineers, assisted by supporting organizations to the S&T and engineering community, are responsible for risk informed protection planning and management of their technology, programs, systems, and technical information to mitigate adversary impacts. Risks include:

(1) Technical Information.

(a) Technical information includes, but is not limited to, classified and unclassified CTI about DoD sponsored research, technology, programs, and systems being acquired, such as:

1. Planning data.

2. Requirements data.

3. Design data.

4. Test data.

5. Operational software data.

6. Support data (e.g., training, maintenance data).

(b) Unclassified information that alone might not be damaging but, when combined with other CUI, could allow an adversary to:

1. Compromise, counter, clone, or defeat a warfighting capability; or

2. Gain a cost and schedule advantage.

(2) Government Research and Development Laboratories, Federally Funded Research Development Centers (FFRDCs), University Affiliated Research Centers, and Program Organizations.

Poor cybersecurity hygiene, untrained personnel, and operational security practices can be used by threat actors to gain program and system knowledge. This includes:

(a) Insufficient or incorrect:

1. Handling and control of classified and controlled information.

2. Marking and dissemination of technical information.

(b) Inadequate information network security.

(3) Contractors and Personnel.

Contractor facilities (including networks, supply chains, personnel, design, development, test, and production environments) can be used by threat actors to access government research and development and program organizations to steal, alter, or destroy system functionality, information, or technology. This includes:

(a) Research and development, manufacturing, testing, and production organizations.

(b) Prime contractors, subcontractors, and universities supporting those organizations.

(4) Software and Hardware.

Software (including firmware) and microelectronics hardware used in a system or incorporated into spares can be deliberately compromised while in the supply chain with the intent to use these compromises for malicious attacks to trigger future system failures. Undiscovered weaknesses or flaws in system elements containing software or microelectronics (including spares) can provide the foundation for threat actors to defeat fielded systems through cyber-attacks. This includes technology and systems required to accomplish the operational and mission requirements, to include access and availability of advanced and assured microelectronics.

(5) Systems, Enabling Systems, and Supporting Systems.

Test, certification, maintenance, or training systems, equipment, and facilities can be used by threat actors to gain access to system functionality, information, or technology. This includes:

(a) Technology in research and development.

(b) Systems in acquisition.

(c) Enabling systems that facilitate lifecycle activities (e.g., research and development, manufacturing, testing, training, logistics, and maintenance).

(d) Supporting systems that contribute directly to operational functions (e.g., interconnecting operational systems).

(6) System Interfaces.

Poorly configured, inadequately maintained, undocumented, or unprotected network and system interfaces can be used by threat actors to:

(a) Gain unauthorized system access; or

(b) Deliver cyber-attacks in the form of malicious software or content.

(7) Fielded Systems.

The supply chain can expose system functionality to unauthorized access that threat actors can potentially exploit to gain access to system functionality. Battlefield loss and exports can expose U.S.-advanced technology to loss from reverse engineering.

3.3. ACTIVITIES TO MITIGATE ADVERSARY THREATS TO TECHNOLOGY AND PROGRAMS.

S&T managers and engineering teams will employ and tailor S&T and program protection measures. S&T managers and engineering teams will assess technology and program risks and opportunities to determine necessary protections. Protection measures include operations security, information safeguarding, research protection, designed-in system protections, SCRM, software assurance, hardware assurance, anti-counterfeit practices, AT, and program security related and engineering cyber-resilient activities. S&T managers and lead systems engineers will be responsible for the procedures as assigned in this paragraph.

a. Safeguard Information.

To safeguard classified and unclassified CTI—starting with the application of appropriate classification and marking guidance for DoD-sponsored research and program data, with a focus on classified information and DoD CUI, which includes CTI—S&T managers and lead systems engineers will:

(1) Work with security classification guidance authorities to determine classification markings as described in Volume 2 of DoD Manual 5200.01.

(2) Assess the impact of the exposure of the CTI that will be placed on unclassified networks, including:

(a) Information contained in solicitations.

(b) Legally binding agreements.

(c) Technical publications associated with research.

(3) Determine, apply, and direct dissemination and marking statements on technical documents and review for public release, as described in DoDIs 5230.24 and 3200.12.

(4) Establish a strong culture of protection awareness and behavior through training and education in:

(a) S&T.

(b) Program offices.

(c) Universities.

(d) FFRDCs.

(e) Grantees.

(f) Contractors.

(5) Ensure:

(a) Protection of CTI is consistent with Clause 252.204-7012 of the Defense Federal Acquisition Regulation Supplement (DFARS), unless exempted by Clause 252.204-7000(a)(3) of the DFARS.

(b) Requirements as described in DoDI 8582.01 are included in legally binding agreements to include, but not limited to:

1. Grants.

2. Other transaction authority.

3. Small business innovation research and technology transfer.

4. Independent research and development.

5. Cooperative research and development agreements.

6. Educational partnership agreements.

(6) Assess losses associated with cyber incidents reported under contracts that contain:

(a) Clause 252.204–7012 of DFARS; or

(b) Language that meets its intent included in other legally binding agreements.

(7) Encourage FFRDC, university, and industry participation in public and private threat information sharing activities, including the DoD's DIB Cybersecurity Program, to enhance and supplement their capabilities to safeguard DoD information that resides on or transits DIB unclassified information systems.

b. Control DoD-Sponsored Research.

To control DoD-sponsored research involving joint ventures, academic collaborations, international talent recruitment programs, cooperative research partnerships, and outside work opportunities through the appropriate budget activity (BA) selection and choice of performers, S&T managers will:

(1) Use DoD 7000.14-R at project initiation and at each additional funding increment to determine the appropriate BA and the anticipated Technology Readiness Level for the type of work to be performed. This determination will be reviewed and approved by S&T leadership to ensure appropriate BA categorization. Research projects will be reviewed annually, at a

minimum, to ensure the appropriate BA categorization determination throughout the life of the S&T project.

(2) Use relevant security classification guides and BA categorization to inform the performer selection (e.g., DoD laboratories, FFRDCs or University Affiliated Research Centers, universities, industry) for research that involves CTI.

(3) Conduct an initial S&T project risk assessment before project approval and review the risk assessment at least annually to ensure programmatic changes are addressed. The risk assessment will determine the:

(a) Scope of the research project.

(b) Impact of unauthorized disclosure.

(c) Recommended courses of action.

(4) Review research performers for workload conflicts and conflict of interest, as part of the contract, grant, or other instrument award process and annually, at a minimum, thereafter. Standard Form 424, "Research and Related and Senior and Key Person Profile (Expanded) Form," for grant application packages and its associated instructions for completion and submission has been established for this purpose.

(5) Review the security program and practices of the institutions receiving research funding.

c. Design for Security and Cyber Resiliency.

To design, develop, test, and acquire systems that can successfully operate in the face of threats, to include cyber threats, as well as in denied environments, lead systems engineers will:

(1) Include cybersecurity, security, and other system requirements into system performance specifications and product support needs that:

(a) Inform requirements derivation activities using the:

1. Draft or validated capability development document or equivalent capability requirements document.

2. Concept of operations.

3. Operational mode summary.

4. Mission profiles.

(b) Use TAPPs, S&T program protection, and relevant PPPs to inform security design and process requirements, as appropriate.

(c) Ensure that key performance parameters and attributes establish:

1. System survivability and sustainment measures.

2. Information system security measures, such as cryptography and key distribution, based on confidentiality, integrity, and availability needs.

(d) Use requirements derivation methods, such as system modeling and analysis, security use and abuse or misuse cases, criticality analysis, and vulnerability analysis to derive system security and exportability requirements that are sufficient to minimize vulnerabilities introduced by design, implementation, system interfaces, and access points.

(e) Incorporate the derived requirements into the system requirements traceability verification matrix.

(2) Allocate cybersecurity and related system security requirements to the system architecture and design and assess the design for vulnerabilities. The system architecture and design will address, at a minimum, how the system:

(a) Manages access to, and use of, the system and system resources.

(b) Is structured to protect and preserve system functions or resources, such as through segmentation, separation, isolation, or partitioning.

(c) Maintains priority system functions under adverse conditions.

(d) Is configured to minimize exposure of vulnerabilities that could impact the mission, including through application of techniques, such as:

1. Design choice.

2. Component choice.

(e) Monitors, detects, and responds to security anomalies.

(f) Interfaces with the DoD Information Network or other external services.

(3) Ensure cybersecurity and related system security requirements, design characteristics, and verification methods to demonstrate the achievement of those requirements are included in the technical baseline. Maintain bi-directional traceability among requirements throughout the system lifecycle.

(4) Include cybersecurity and related system security in the conduct of technical risk management activities and change management processes to address risk identification, analysis, mitigation planning, mitigation implementation, and tracking. Use evolving technology, program, and system threats to inform operational impacts. The goal is to mitigate risks that could have an impact on meeting performance objectives as well as thresholds. Technical risks, and opportunities as applicable, will:

(a) Be assessed at technical reviews.

(b) Include cost and schedule implications.

(5) Request technology, program, and system threat assessments from appropriate intelligence, counterintelligence, and security entities to continuously assess risks to the technology, programs, and the system.

(6) Identify and protect capabilities contributing to the warfighters' technical advantage, throughout the lifecycle, in accordance with DoDD 5200.47E. S&T managers and lead systems engineers will:

(a) Apply DoD horizontal protection guidance to determine requirements for planning, designing, implementing AT and exportability features, as appropriate, to technology and systems when outside of U.S. control.

(b) Coordinate with the applicable DoD Component office of primary responsibility for DoD AT to coordinate activities to mitigate reverse engineering opportunities, where appropriate.

(7) Use assured suppliers or appropriate SCRM countermeasures for system elements that perform mission-critical functions, in accordance with DoDI 5200.44. No source may be excluded from a procurement based upon SCRM consideration absent proper exercise of appropriate legal authority. Any such exclusion must be coordinated with and approved by the contracting officer and Counsel. Technical mitigations for mission-critical functions and critical components must, at a minimum, include:

(a) Software assurance.

(b) Hardware assurance.

(c) Procurement strategies.

(d) Anti-counterfeit practices.

(8) Use validated cybersecurity solutions, products, and services when available and cost effective, in accordance with DoDI 8500.01.

(9) Request assistance, when appropriate, from the JFAC, established in accordance with DoD Policy Memorandum 15-001, to support software and hardware assurance requirements.

(10) Implement:

(a) A process for the identification and prioritization of security vulnerabilities, based on risk.

(b) Appropriate remediation strategies for such security vulnerabilities.

(11) Incorporate automated software vulnerability analysis tools throughout the lifecycle of the system, including during development, operational test, operations and sustainment phases, and retirement, to:

(a) Evaluate software vulnerabilities.

(b) When appropriate, use software vulnerability analysis enterprise licenses provided by the JFAC.

(12) Translate S&T protection and program protection, including software and hardware assurance remediation strategies, into contract requirements.

d. Protect the System Against Cyber Attacks from Enabling and Supporting Systems.

S&T managers and lead systems engineers will:

(1) Identify all system interfaces to all enabling and supporting systems and assess cybersecurity vulnerabilities. S&T managers and lead systems engineers will review vulnerabilities introduced by enabling and supporting systems and support activities, including:

(a) Engineering, simulation, and test tools and environments.

(b) Third party certification and assessment activities.

(c) Logistics, maintenance, and training support activities.

(d) All interoperable or ancillary equipment that the system operates or with which it interfaces.

(2) Use threat intelligence from the Defense Intelligence Agency, DoD Component intelligence and counterintelligence activities, the Defense Counterintelligence and Security Agency, and the Joint Acquisition Protection and Exploitation Cell to assess third party service providers and environments (e.g., training, testing, logistics, or certification).

e. Protect Fielded Systems.

S&T protection and program protection measures implemented during concept development, engineering, and test activities do not ensure security is maintained throughout operations. Program protection requirements evolve as technology and threats evolve. Once technology and systems are fielded, they become exposed to a changing threat environment and potentially different vulnerabilities. Planning for maintaining appropriate technology and system security must be considered early and throughout the lifecycle. S&T managers and lead systems engineers will:

(1) Conduct periodic reassessments of technology and system security vulnerabilities to the technology, system, and support systems. These reassessments must be conducted, at a minimum, for any engineering modifications or technology refreshes. Technical and process

mitigations will be incorporated into engineering, test, and logistics documentation, and related solicitations, contracts, and other legal binding agreements.

(2) Ensure technology, program, and system information is protected and the process for identification, prioritization, and mitigation of weaknesses and vulnerabilities, including use of automated tools, remains consistent from development to sustainment to minimize vulnerabilities introduced by depot and other sustainment activities (e.g., training, maintenance manuals, and supply).

(3) Monitor considerations for AT protections that are implemented in fielded systems.

f. Enhance Protection for Critical Programs and Technologies.

S&T managers and lead systems engineers should employ risk informed enhanced protection measures to mitigate targeted threats and vulnerabilities in selected technologies and programs. S&T managers and lead systems engineers will engage with security, counterintelligence, and intelligence resources to inform:

(1) Design development.

(2) Supply chain.

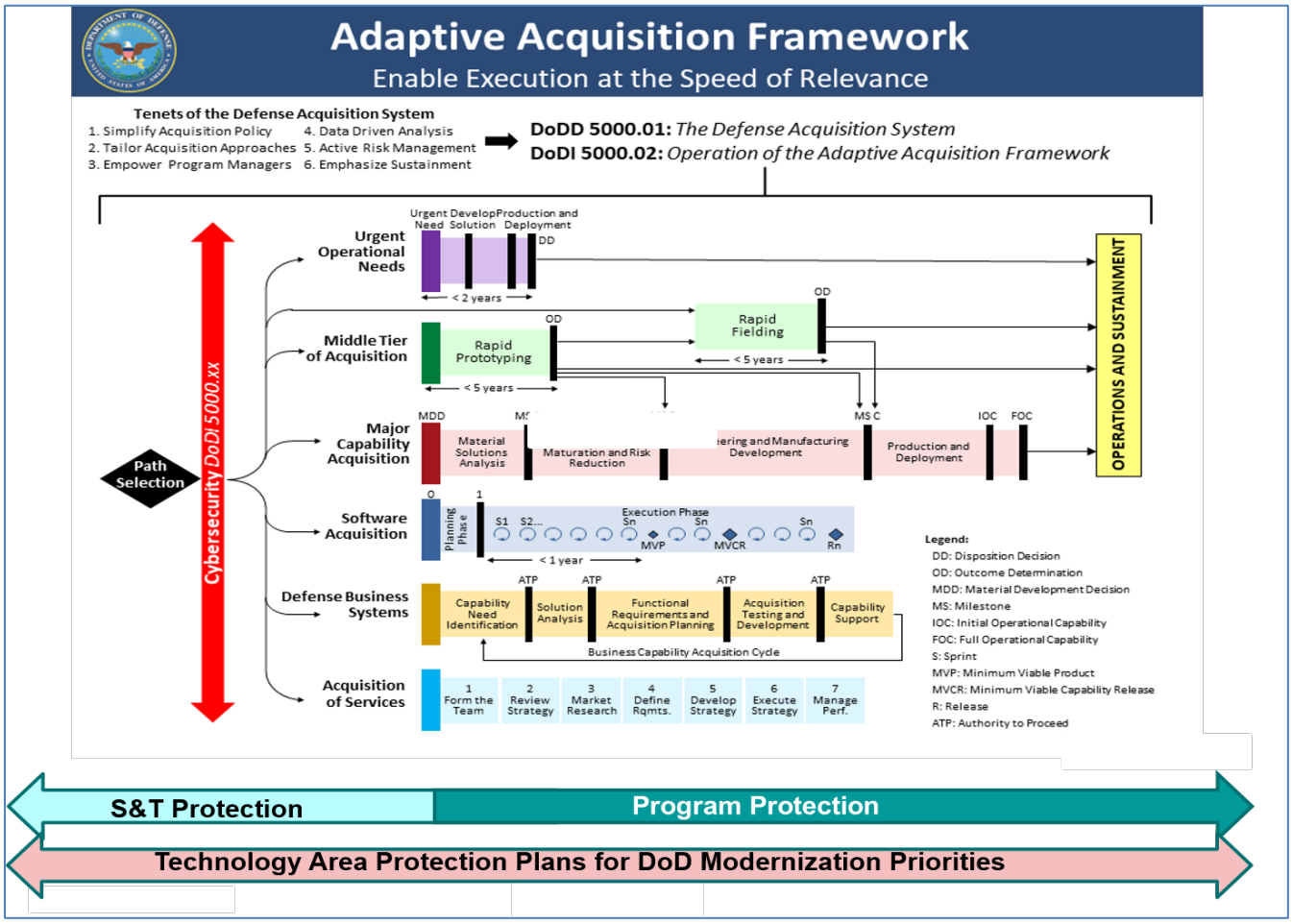
(3) Program management risk decisions.

(4) Procurement actions.

3.4. TECHNOLOGY AND PROGRAM PROTECTION MANAGEMENT.

Management of TAPPs, S&T protection plans, and PPP across the lifecycle is shown in Figure 1.

Figure 1. Technology and Program Protection Framework



a. TAPP.

A TAPP will be established for each S&T modernization priority area. The TAPP will inform S&T research at the appropriate BA level, or at Technology Readiness Levels 1-6 and PPPs. The TAPP is designed to reduce compromise or loss of critical technologies and protect against unwanted technology transfer. In addition, it will guide DoD:

(1) S&T.

(2) Export controls.

(3) International agreements.

(4) Security.

(5) Counterintelligence.

(6) Law enforcement activities.

b. S&T Protection Plans.

S&T managers will prepare protection plans as a management tool to guide S&T protection activities. S&T projects, when associated with critical technology or modernization priority areas, will be consistent with their applicable TAPPs and all available horizontal protection guidance.

(1) At a minimum, the S&T protection plan will include:

(a) Critical technology elements and enabling technologies.

(b) Threats to, and vulnerabilities of, these items.

(c) Selected countermeasures to mitigate associated risks.

(2) The S&T protection plan will be submitted for approval before project approval and at intervals as defined by the DoD Component.

(a) S&T managers should:

1. Ensure S&T protection requirements are included in solicitations, broad agency announcements, as well as legally binding agreements resulting therefrom.

2. Prepare updates to the S&T protection plan:

a. After an approved technical approach.

b. Upon identification of any significant threat activity or compromise.

(b) S&T managers will transition the S&T protection plan to the lead systems engineer responsible for system development when:

1. A technology transition decision has been made.

2. Technology transfer requirements have been met to inform the PPP.

c. PPP.

Lead systems engineers will prepare a PPP as a management tool to guide the systems security engineering activities, to include cyber resilient engineering, across the lifecycle.

(1) At a minimum, the PPP will include the:

(a) Plan to apply countermeasure as described in the PPP outline and guidance template to mitigate associated risks.

(b) Threats to, and vulnerabilities of, these items.

(c) Planning for exportability and potential foreign involvement.

(2) The PPP will be submitted for approval, in accordance with Major Capability Acquisition, Operation of Middle Tier Acquisition, Urgent Operation Needs, and Software Acquisition at each acquisition pathway decision points. The cybersecurity strategy will be submitted as an appendix, in accordance with DoDI 5000.82.

(a) For all programs where the DAE is the milestone decision authority, the USD(R&E) is the PPP approval authority.

(b) Lead systems engineers should ensure the appropriate PPP countermeasures and cyber resilient engineering requirements are included in request for proposals and prepare updates to the PPP after:

1. Any contract award to reflect the contractor's approved technical approach.

2. Identification of any significant threat activity or compromise.

(3) Program protection planning responsibilities will transition over the lifecycle. After the full-rate production or full-deployment decision, the PPP will transition to the program manager responsible for system sustainment and disposal.

d. Independent Technical Risk Assessments.

Refer to DoDI 5000.88 for requirements to conduct and approve independent technical risk assessments on system designs and interfaces for adversarial risks, program protection, and cyber vulnerabilities. The results must inform technical baselines and risk management activities.

e. System Engineering Plan.

Refer to DoDI 5000.88 for engineering activities and technical approaches that support program protection planning.

f. Test and Evaluation Master Plan.

Refer to DoDI 5000.89 for:

(1) Development, test, and evaluation.

(2) DoD operational test and evaluation system security and cybersecurity engineering activities that support program protection planning.

g. Life-Cycle Sustainment Plan.

Refer to DoDI 5000.02 for life-cycle sustainment system security and cybersecurity engineering activities that support protection planning.

3.5. TAILORED PROGRAM PROTECTION FOR SELECTED ACQUISITION PATHS.

Engineers will tailor program protection strategies and oversight, content, timing and scope of countermeasures, based on the characteristics of the capability being acquired, including complexity, risk, and urgency to satisfy user requirements.

a. Major Capability Acquisition.

In accordance with DoDI 5000.02, S&T managers and lead systems engineers will:

(1) Use relevant:

(a) TAPPs to inform program protection activities, as appropriate.

(b) S&T protection plans, as appropriate.

(2) Develop program protection planning and implementation as part of the design and technical risk assessment process.

(3) Ensure operators are informed of operational risks when the system is fielded.

b. Urgent Capability Acquisition.

In accordance with DoDI 5000.81, S&T managers and lead systems engineers will:

(1) Use relevant:

(a) TAPPs to inform program protection activities, as appropriate.

(b) S&T protection plans, as appropriate.

(2) Develop program protection planning and implementation as part of the design and technical risk assessment process.

(3) Ensure operators are informed of operational risks when the system is fielded.

c. Operation of the Middle Tier of Acquisition.

In accordance with DoDI 5000.80, S&T managers and lead systems engineers will:

(1) Determine program protection planning and implementation risks and mitigation as part of the design and technical risk assessment process.

(2) Ensure operators are informed of the operational risks when the system is fielded.

d. Software Acquisition.

In accordance with DoDI 5000.87, S&T managers and lead systems engineers will:

(1) Consider mitigations that promote automated continuous integration and continuous delivery for adoption of agile, lean, or development security operations methodologies to determine:

(a) Program protection planning.

(b) Implementation risks.

(2) Ensure operators are informed of the operational risks when the system is fielded.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
ACAT	acquisition category
AT	anti-tamper
BA	budget activity
CTI	controlled technical information
CUI	controlled unclassified information
DAE	defense acquisition executive
DAS	Defense Acquisition System
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DoDD	DoD directive
DoDI	DoD instruction
FFRDC	federally funded research and development center
JCIDS	Joint Capability Integration and Development System
JFAC	Joint Federated Assurance Center
PPP	program protection plan
S&T	science and technology
SCRM	supply chain risk management
TAPP	technology area protection plan
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(R&E)	Under Secretary of Defense for Research and Engineering

G.2. DEFINITIONS.

Unless otherwise noted, a complete glossary of the terms used in this issuance is maintained on the Defense Acquisition University Website at https://www.dau.edu/.

TERM	DEFINITION
horizontal protection	Defined in DoDI 5200.39

REFERENCES

Defense Federal Acquisition Regulation Supplement, current edition

Directive-type Memorandum S-DTM-19-005, "(U) Nuclear Command, Control, and Communications Enterprise Governance," April 17, 2019, as amended

DoD 7000.14-R, "Department of Defense Financial Management Regulation (FMR)," date varies by volume

DoD Directive 5000.01, "The Defense Acquisition System," September 9, 2020

DoD Directive 5105.42, "Defense Security Service (DSS)," August 3, 2010, as amended

DoD Directive 5111.01, "Under Secretary of Defense for Policy (USD(P))," June 23, 2020

DoD Directive 5137.02, "Under Secretary of Defense for Research and Engineering (USD(R&E))," July 15, 2020

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Directive 5200.47E, "Anti-Tamper (AT)," September 4, 2015, as amended

DoD Instruction 3200.12, "DoD Scientific and Technical Information Program (STIP)," August 22, 2013, as amended

DoD Instruction 5000.02, "Operation of the Adaptive Acquisition Framework", January 23, 2020

DoD Instruction 5000.02T, "Operation of the Defense Acquisition System," January 7, 2015, as amended

DoD Instruction 5000.80, "Operation of the Middle Tier of Acquisition (MTA)," December 30, 2019

DoD Instruction 5000.81, "Urgent Capability Acquisition," December 31, 2019

DoD Instruction 5000.82, "Acquisition of Information Technology", April 21, 2020

DoD Instruction 5000.87, "Operation of the Software Acquisition Pathway," October 2, 2020

DoD Instruction 5000.88, "Engineering of Defense Systems," November 18, 2020

DoD Instruction 5000.89, "Test and Evaluation," November 19, 2020

DoD Instruction 5200.39, "Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E), May 28, 2015, as amended

DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012, as amended

DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)", March 6, 2020

DoD Instruction 5205.13, "Defense Industrial Base (DIB) Cybersecurity (CS) Activities," January 29, 2010, as amended

DoD Instruction 5230.24, "Distribution Statements on Technical Documents," August 23, 2012, as amended

DoD Instruction 5230.27, "Presentation of DoD-Related Scientific and Technical Papers at Meetings," November 18, 2016, as amended

DoD Instruction 5530.03, "International Agreements," December 4, 2019

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction 8582.01, "Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information," December 9, 2019

DoD Instruction O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011, as amended

DoD Manual 5200.01, Volume 2, "DoD Information Security Program: Marking of Information," February 24, 2012, as amended

DoD Manual 5220.22, Volume 2, "National Industrial Security Program: Industrial Security Procedures for Government Activities," August 1, 2018, as amended

DoD Policy Memorandum 15-001, "Joint Federated Assurance Center (JFAC) Charter," February 9, 2015

Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended

Public Law 112-239, Section 933, "National Defense Authorization Act for Fiscal Year 2013," January 2, 2013

Public Law 113-66, Section 937, "National Defense Authorization Act for Fiscal Year 2014," December 26, 2013

Public Law 115-232, "John McCain National Defense Authorization Act for Fiscal Year 2019," August 13, 2018

United States Code, Title 10, Section 133a