BY ORDER OF THE
SECRETARY OF THE AIR FORCE

DoDI5000.83_DAFI63-113

8 MARCH 2022

Acquisition / Logistics

TECHNOLOGY AND PROGRAM PROTECTION TO MAINTAIN TECHNOLOGICAL ADVANTAGE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: **Publications and forms are available on the e-Publishing website at www.e-publishing.af.mil for downloading or ordering.**

RELEASABILITY: **There are no releasability restrictions on this publication.**

OPR: SAF/AQXS

Certified by: SAF/AQX
(Mr. William Bailey)

Supersedes: AFPAM 63-113, 17 October 2013

Pages: 49

This Supplement implements Air Force Policy Directive (AFPD) 63-1/20-1, *Integrated Life Cycle Management.* This supplement also implements Air Force Instruction (AFI) 63-101/20-101, *Integrated Life Cycle Management*, Department of Defense (DoD) Instruction (DoDI) 5000.83, *Technology and Program Protection to Maintain Technological Advantage*, DoD Directive (DoDD) 5000.47E, *Anti-Tamper (AT)*, DoDI 5200.39, *Critical Program Information (CPI) Identification and Program Protection Within Research, Development, Test and Evaluation (RDT&E)*, DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*. This supplement also provides United States Air Force (USAF) and United States Space Force (USSF) with guidance for technology and program protection. The DoDI is printed word-for-word in regular font without editorial review. Department of the Air Force (DAF) supplementary material is printed in bold font and indicated by "(Added)(DAF)." This publication applies to individuals at all levels who research, develop, test, review, approve, or manage systems, subsystems, end-items, services, and activities throughout the system engineering lifecycle (for the purpose of this publication referred to as "technological and programs protection" throughout this document) and applies to acquisition efforts. This guidance implements acquisition security, a key element of program protection, for Air Force programs. Ensure that all records generated as a result of processes prescribed in this publication adhere to AFI 33-322, *Records Management and Information Governance Program*, and disposed of in accordance with Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. This publication may be supplemented at any level, but all supplements must be routed to the Deputy Assistant Secretary (Acquisition Integration) (SAF/AQX), for review and approval prior to publication. (T-1). Send all recommended changes or comments about this publication to SAF/AQX, at SAF.AQ.SAF-AQXS.Policy.Workflow@us.af.mil, through the appropriate functional chain of command using AF Form 847, *Recommendation for Change of Publication*. The

authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See DAFI 33-360, *Publications and Forms Management*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor's commander for non-tiered compliance items.

SUMMARY OF CHANGES

This publication changes Air Force Pamphlet (AFPAM) 63-113 to a DAFI and serves as the Department of the Air Force Supplement to DoDI 5000.83, *Technology and Program Protection to Maintain Technological and Advantage*. It supersedes the AFPAM 63-113 with changes that include program start date, entrance and exit documentation requirements, approval authority, and guidance to maintain program technology and program protection.

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
Change 1 Effective:	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:	Michael D. Griffin, Under Secretary of Defense for Research and Engineering
Change 1 Approved by:	Barbara K. McQuiston, Performing the Duties of Under Secretary of Defense for Research and Engineering

ANDREW P. HUNTER
Assistant Secretary of the Air Force
(Acquisition, Technology & Logistics)

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.

(6) **(Added)(DAF) Research and development.**

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. **(Added)(DAF) Research and development and protection of intellectual property should also be considered when establishing risks for adversarial exploitation and compromise.**

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.

(1) (Added)(DAF) Programs will also employ digital engineering practices and methodologies, Development, Security and Operations (DevSecOps), and Modular Open

Systems Approach (MOSA) into program protection review and analysis to the maximum extent possible. (T-1)

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.

e. (Added)(DAF) See DAFI 61-201, *Management of Scientific and Technical Information (STINFO)*, for additional information on how to protect S&T information.

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

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/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 (USD(I&S)).

In accordance with DoDD 5143.01, the USD(I&S):

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.

(a) (Added)(DAF) S&T Protection Plans are developed for DAF S&T programs.

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

(a) (Added)(DAF) S&T Protection Plans are approved by the decision 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. **(Added)(DAF) S&T, PPPs, and planning activities will reference the Critical Program and Technology List to prioritize effort. (T-1)**

(4) (Added)(DAF) PPPs will be developed for non-ACAT programs such as demonstrations and prototypes. (T-1) Refer to the following reference for more information.

https://www.dau.edu/cop/pm/_layouts/15/WopiFrame.aspx?sourcedoc=/cop/pm/DAU%20Sponsored%20Documents/PPP%20Outline%20and%20Guidance%20v1%20July2011.pdf&action=default&DefaultItemOpen=1

c. (Added)(DAF) Threats from foreign influence / foreign control are mitigated when acquisition-related company products and services under foreign ownership, control, or influence are avoided or closely monitored.

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.

2.8. (Added)(DAF) THE ASSISTANT SECRETARY OF THE AIR FORCE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS (SAF/AQ), as the Component Acquisition Executive (CAE) for the Air Force and the ASSISTANT SECRETARY OF THE AIR FORCE FOR SPACE ACQUISITION AND INTEGRATION (SAF/SQ) as the CAE for space systems and programs (effective when assigned, no later than 1 OCT 22) will:

(Added)(DAF) (Note: The term Service Acquisition Executive (SAE) is equivalent to the term Component Acquisition Executive used in DoD directives and instructions.)

a. (Added)(DAF) Provide guidance and oversight for acquisition security activities.

b. (Added)(DAF) Delegate to a Decision Authority (DA) for supported acquisition security activities per this instruction, with further delegation allowed as identified in AFI 63-101/20-101, Integrated Life Cycle Management. Note: DA may also be referred to as Milestone Decision Authority.

c. (Added)(DAF) Designate the Assistant Secretary for Science, Technology and Engineering (SAF/AQR) as the office responsible for system engineering, and reviewing and validating PPPs. SAF/AQR is also the Department of the Air Force Secretariat for developing and maintaining the Air Force Critical Program and Technology List.

d. (Added)(DAF) Designate the Cyber Resilient Office for Weapons Systems (CROWS) as the office for developing system security engineering and PPP tools, methods, and practices in support of acquisition programs.

e. (Added)(DAF) Designate the Chief Software Office (SAF/CSwO) as the office responsible for directing DevSecOps services for DAF programs.

f. (Added)(DAF) Designate the Deputy Assistant Secretary for Acquisition Integration (SAF/AQX) as the office responsible for the review, investigation and adjudication of potential Committee on Foreign Investments in the United States cases received from the Office of the Secretary of Defense, Foreign Investment Risk. Foreign influence / foreign control is mitigated when acquisition related company products and services may be at risk of foreign ownership, control, or influence. (T-0) Additionally, to ensure compliance, SAF/AQX participates in monitoring National Security Agreements in which DAF is party or has a significant interest to ensure compliance.

g. (Added)(DAF) Ensure Decision Authorities and Program Managers implement trusted systems and network policy per DoDI 5200.44 and cybersecurity per DoDI 5000.90, *Cybersecurity for Acquisition Decision Authorities and Program Managers.* (T-0)

h. (Added)(DAF) Designate the Deputy Assistant Secretary for Special Programs (SAF/AQL) as the Office of Primary Responsibility for reviewing and validating anti-tamper (AT) plans.

2.9. (Added)(DAF) THE DEPUTY CHIEF OF STAFF FOR STRATEGY, INTEGRATION, AND REQUIREMENTS (AF/A5) will:

a. (Added)(DAF) Support development of acquisition security requirements for programs.

b. (Added)(DAF) Provide a streamlined process for requirements approval.

c. (Added)(DAF) Ensure that acquisition security requirements in development documents address both current and projected ten year threats relative to acquisition attack surfaces, which include system hardware and software vulnerabilities, supply chain, development environments, data at rest and data in motion, insider threats, and testing (collection on open testing, as an example).

2.10. (Added)(DAF) THE DEPUTY CHIEF OF STAFF FOR PLANS AND PROGRAMS (AF/A8) will perform planning and programming for acquisition security activities.

2.11. (Added)(DAF) THE DIRECTOR, AIR FORCE TEST AND EVALUATION (AF/TE) will:

a. (Added)(DAF) Provide guidance, direction, and oversight for all matters pertaining to the formulation, review, and execution of test and evaluation plans, policies, programs, and budgets, which may include acquisition security activities.

b. (Added)(DAF) Act as the final DAF review authority and signatory for Master Test Plans or Test and Evaluation Master Plan or other test strategy documentation prior to Air Force or Space Force SAE (effective 1 Oct 2022) approval and signature, ensuring acquisition security, PPP, DevSecOps and MOSA requirements are planned, resourced, and evaluated. AF/TE will approve/sign Test and Evaluation Master Plans for any program on DOT&E oversight.

c. (Added)(DAF) Manages the Air Force test infrastructure for the DAF in cooperation with Space Force Test and Evaluation (SF/TE) to ensure adequate facilities, resources, and expertise are available to support system life cycle test and evaluation activities.

2.12. (Added)(DAF) ADMINISTRATIVE ASSISTANT SECRETARY TO THE SECRETARY OF THE AIR FORCE (SAF/AA).

a. (Added)(DAF) Responsible for oversight and implementation of personnel security, industrial security, and information security programs including the Air Force Insider Threat Program, Special Access Programs, and CUI programs.

2.13. (Added)(DAF) THE ASSISTANT SECRETARY OF THE AIR FORCE FOR FINANCIAL MANAGEMENT (SAF/FM).

a. (Added)(DAF) Advise the acquisition security activities in accordance with responsibilities contained within DAFMAN 65-605, *Budget Guidance and Technical Procedures, Volume 1*, paragraphs 1.3.3. and 2.1., as further articulated in Air Force Policy Directive (AFPD) 90-6, *Air Force Strategy, Planning, Programming, Budgeting, and Execution (SPPBE) Process*.

b. (Added)(DAF) Incorporate technical content from approved TAPP, S&T protection plan, and PPP to support approved acquisition security processes during development of the Service Cost Position or a Non-Advocate Cost Assessment as required by AFI 65-508, *Cost Analysis Guidance and Procedures*.

2.14. (Added)(DAF) CHIEF INFORMATION OFFICER (SAF/CN).

a. (Added)(DAF) Responsible for tracking system authorizations, enterprise architecture, and Clinger-Cohen Act compliance.

2.15. (Added)(DAF) THE CHIEF DATA OFFICER (SAF/CO).

a. (Added)(DAF) Responsible for setting data standards and managing the implementation of sharable data and services to support acquisition security within the DAF and its military counterparts.

2.16. (Added)(DAF) THE DECISION AUTHORITY (DA).

a. (Added)(DAF) Certify program decision points for entry and exit criteria meet established program requirements that includes a status and risk assessment of program acquisition security and program decision points consider program risks for technology and program threats. (T-1)

b. (Added)(DAF) Ensure acquisition pathway programs are included in the Investment Master List or the Acquisition Master List. (T-1)

c. (Added)(DAF) Resolve horizontal protection issues that impact one or more programs outside of the DA purview. (T-1)

2.17. (Added)(DAF) PROGRAM MANAGERS.

a. (Added)(DAF) Document that security-related requirements are fully derived for the system and for supporting infrastructure.

b. (Added)(DAF) Ensure security-related requirements are included in request for proposal contract language and in source selection criteria where appropriate to include security considerations at the prime and subcontractor locations. (T-1)

c. (Added)(DAF) Protect Critical Program Information and mission-critical functions and components, ensuring their protection to keep technological advantages in and malicious content out by ensuring horizontal identification and protection utilizing the acquisition security database when conducting horizontal identification and protection analysis. (T-0)

d. (Added)(DAF) Oversee completed Program Protection Plans are included the System Engineering Plan then transferred to the Life Cycle Sustainment Plan when a program transitions into Operations and Sustainment phase. (T-0)

e. (Added)(DAF) Validates that appropriate countermeasures are implemented to mitigate insider threat risk when contractor owned/contractor operated depots are utilized for sustainment efforts or outside the Continental United States fielded systems. (T-1)

f. (Added)(DAF) Will notify the decision authority or Chief Information Officer (CIO) when a high risk cannot be addressed and document them in the Program Protection Plan or S&T Protection Plan. (T-1)

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.

c. (Added)(DAF) Technology and program protection will also tailor in for the following: communications security; biometric countermeasures; and anti-tamper countermeasures. (T-0)

d. (Added)(DAF) Special Access Programs created under the authority of Executive Order 13526, *Classified National Security Information*, are exempt from compliance in developing a Program Protection Plan. (T-0) This exemption does not include anti-tamper plans or the Cybersecurity Strategy. (T-1) The Program Manager collaborates with SAF/AAZ when Special Access Program information is involved to determine a prudent protection approach prior to developing a Program Protection Plan. (T-1)

e. (Added)(DAF) Nuclear components governed by DoDM 5030_AFMAN 63-103, *DoD Procedures for Joint DoD-Department of Energy/National Nuclear Security Administration (DOE/NNSA) Nuclear Weapon Life-Cycle Activities*, and DOD-DOE or Air Force-National Nuclear Security Administration (AF – NNSA) agreements are not exempt from system security considerations. (T-1) The Program Manager is responsible to ensure Nuclear weapons security is accomplished consistent with DoDD 3150.02, *DoD Nuclear Weapons Surety Program,* and nuclear surety tamper control and detection in consistent with AFI 91-101, *Air Force Nuclear Weapons Surety Program.* (T-0)

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.

(a) (Added)(DAF) Programs and S&T should also be vigilant for counterfeit or alternated components introduced to the supply chain as products and services are acquired. Intelligence and counterintelligence professionals will be consulted to provide current threat information to the program supply chain risk management process. (T-0)

(b) (Added)(DAF) Inherited Critical Program Information is identified and properly documented in the Program Protection Plan. Inherited Critical Program Information responsibilities extend across a program's entire lifecycle protected by using the following countermeasures: communication security, biometric security, and anti-tamper.

(4) Subvert or compromise DoD:

(a) Technology;

(b) Systems;

(c) Enabling systems; or

(d) Support systems.

(5) (Added)(DAF) Foreign military sales and direct commercial sales programs must implement program protection and other security considerations. (T-1)

(a) (Added)(DAF) The Program Manager summaries international activities, to include plans for foreign cooperative development or foreign sales, or reasonable probability for future foreign cooperative development or sales, in the Program Protection Plan. Identified Critical Protection Information, countermeasures, designs, testing, and acquisition documents should be consistent with foreign involvement. (T-1)

(b) (Added)(DAF) The Program Manager ensures that defense exportability features are incorporated into the requirements development and engineering processes and that appropriate countermeasures are included in the Program Protection Plan. (T-1) The Program Manager includes links to relevant defense exportability features discussions

in the Acquisition Strategy. See DoDI 2010.06, *Materiel Interoperability and Standardization with Allies and Coalition Partners,* for more information.

(c) (Added)(DAF) The Security Assistance Program Manager ensures organizations and foreign recipients establish plans and procedures that foster compliance with the security cooperation process to mitigate risks associated with continued Critical Program Information disclosure during an international transfer conducted via Direct Commercial Sale or Foreign Military Sales in accordance with AFMAN 16-101, *Security Cooperation (SC) and Security Assistance (SA) Management.* (T-1) The Security Assistance Program Manager assesses proposed technology or information to be shared with foreign partners and validates whether the foreign partner security protection capabilities are consistent with providing protection at substantially the same degree of security as the U.S.

(d) (Added)(DAF) Critical Program Information is released to foreign entities (e.g., government military business) only after appropriate reviews (e.g., International Traffic in Arms Regulation) and approvals (Foreign Disclosure Office in accordance with DAFMAN 16-201, *Air Force Foreign Disclosure and Technology Transfer Program*. (T-0) Safeguards must exist for continued Critical Program Information disclosure prevention after given to the foreign entities. (T-1)

(6) (Added)(DAF) Provision provided in the Defense Production Act of 1950 (50 United States Code [USC] App Section 2061 et seq.) and Federal Acquisition Regulation (FAR) subpart 11.602 allow for prioritized delivery of goods, industrial base security, and protection from foreign acquisition for critical industry for national security needs. Program Managers with inquiries or concerns involving any of these industrial base risks can direct their questions to SAF/AQX's Industrial Liaison Branch (SAF.AQ.SAF-AQXE.Industrial.Liaison.Wkflw@us.af.mil).

(a) (Added)(DAF) Defense Production Act Title I (Defense Priorities and Allocation Systems [DPAS]). The Program Manager can recommend, via Title I of the Defense Production Act, a program for a rated order or Special Priorities Assistance under the DPAS Regulation (15 Code of Federal Regulations [CFR] 700). Rated orders are a strategic tool that may compete with other DAF or DoD deliveries, not just commercial orders, and must be considered holistically against other rated orders. The Program Manager's recommendation is routed to SAF/AQX's Industrial Liaison Branch which coordinates with Air Force Materiel Command's DPAS office.

1. (Added)(DAF) BIS-999, *Request for Special Priorities Assistance*, is completed by the program manger. Special Priorities Assistance can be used to expedite product (i.e., component level) delivery to meet a special date or to accelerate delivery under a rated order due to a change in military urgency. It can also be used to resolve delivery conflicts among various priority rated orders.

2. (Added)(DAF) DD Form 691, *Application for Priority Rating for Production or Construction Equipment*, is completed by the Program Manager. Defense orders (i.e., acquisition program level) are assigned an industrial priority rating of either "DO" (i.e., priority) or "DX" (i.e., highest priority). The "DX" rating is authorized by the

Secretary of Defense for program of the highest national urgency. The priority rating cascades from the prime contractor down through all subcontractors. A rated order placed with a supplier takes precedence over all non-rated orders and must be filled ahead of the non-rated orders as needed to meet required delivery dates to resolve DPAS violations, interagency or joint conflicts, and routing for BIS-999. (T-1)

3. (Added)(DAF) Contracting Officers apply priority ratings to contracts according to DoD 4400.01-M, *Priorities and Allocation Manual*. (T-0)

7. (Added)(DAF) The Program Manager can recommend expansion of critical productive capacity and supply by employing authorities contained in Title III of the DPA. These authorities include direct investments necessary to create, sustain (i.e., Diminishing Manufacturing Sources/Material Shortages), expedite, expand, protect, or restore critical industrial capacities or services essential to the national defense. The Secretary of the AF is designated the sole and exclusive DoD Executive Agent with responsibility for DPA Title III Program execution. Air Force Research Laboratory Commander (AFLC/CC) is responsible for establishing and operating a Title III Executive Agent Program Office that is situated within its AFRL/RX Directorate. Program Manager recommendations are routed to AFRL) with a copy to the Deputy Assistant Secretary of Defense for Industrial Policy Title III Director and SAF/AQX's Industrial Liaison Branch.

8. (Added)(DAF) DPA Title VII Committee on Foreign Investment in the United States. Per DoDI 2000.25, *DoD Procedures for Reviewing and Monitoring Transactions Filed with the Committee on Foreign Investment in the United States (CFIUS)*, the AF is a primary stakeholder for DoD CFIUS reviews. Responsibility for DPA Title VII is delegated to SAF/AQX, which appoints the Committee on Foreign Investment in the United States focal point for the AF. The program manager's recommendation, concern, or inquiry is routed to the AF Committee on Foreign Investment in the United States focal point (SAF.AQ.SAF-AQXE.Industrial.Liaison.Wkflw@us.af.mil).

a. (Added)(DAF) When a program, or part of its supply chain, is at risk to (or is dependent on) a foreign person or organization's purchase, merger, or otherwise obtaining significant control of a necessary supplier, U.S. business, or asset, the Program Manager provides acquisition risk (or benefit) information to the AF Committee on Foreign Investment in the United States focal point.

b. (Added)(DAF) If a Program Manager is tasked to provide information to the AF Committee on Foreign Investment in the United States focal point during the course of an investigation, it must be relevant and timely to the prescribed deadlines as there are statutory timelines associated with initial review and investigation phases. (T-1)

9. (Added)(DAF) The Program Manager participates in National Interest Determination activities in connection with Foreign Ownership, Control, or Influence situations when a US prime or subcontractor, cleared under a special security agreement and determined to be operating under foreign ownership, control or influence, requires access to proscribed information (Top Secret, Special Access Program, Secret Compartmented Information, Communication Security, and Restricted Data). National

Interest Determination implementation is consistent with DoDI National Industrial Security Program (NISP), DoDM 5220.22 Vol. 2, *National Industrial Security Program Operating Manual*, and DoDM 5220.22 Vol. 3, *National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI)*. See AFI 16-1406, *Air Force Industrial Security Program*, AFI 16-701, *Management, Administration and Oversight of Special Access Programs*, and Directive-type Memorandum (DTM) 15-002, *Policy Guidance for the Processing of National Interest Determinations (NIDWS) in Connection with Foreign Ownership, Control, or Influence (FOCI)* for more information.

10. (Added)(DAF) Supply Chain Risk Management. The systematic process for managing risk by identifying, assessing, and mitigating actual or potential threats, vulnerabilities, and disruptions to the AF supply chain from beginning to end to ensure mission effectiveness. Successful supply chain risk management maintains the integrity of products, services, people, and technologies; and ensures the undisrupted flow of product, materiel, information, and finances across the lifecycle of a weapon or support system. Addresses the broad spectrum of supply chain risks that have the potential to jeopardize the integrity of assets, compromise intellectual property, disrupt the flow of crucial goods or services needed for continued AF operations, or drive materiel cost increases to the program. Potential supply chain risks include, but are not limited to, technology risks, counterfeit parts, diminishing manufacturing sources and material shortages, quality risks, financial risks, political and regulatory risks, foreign influence risks, operational risks, environmental risks, and human capital risks.

(a) (Added)(DAF) USSF and Air Force Materiel Command identify Supply Chain Risk Management Focal Points to act as the clearinghouse for supply chain risk management data and information. The focal points will:

1. (Added)(DAF) Collect, integrate, analyze, synchronize, and monitor enterprise supply chain risk data and efforts. (T-1)

2. (Added)(DAF) Support supply chain risk management by providing direct assistance to Program Managers, to include program reviews, as requested. (T-3)

3. (Added)(DAF) Provide periodic briefings and elevate enterprise risks on supply chain risk management activities to SAF/AQD, including other HAF agencies when appropriate. (T-2)

11. (Added)(DAF) Countermeasures. The PM uses countermeasures to protect critical and sensitive aspects of the program to include Critical Program Information, classified, critical unclassified information, hardware and software, cyber, within both industry and the government. The protection is applied at the appropriate security classification level as identified in the program's Security Classification Guide under Cryptographic Countermeasures. (T-0). Cryptographic countermeasures are developed in accordance with DoDM 5220.22, National Industrial Security Program Operating Manual; DoDM 5220.22, Vol. 2 *National Industrial Security Program: Industrial Security Procedures for Government Activities*; DoDI 8500.01, DoDI 8520.02, *Public Key Infrastructure (PKI) and*

***Public Key (PK) Enabling*; DoDI 8520.03, *Identify Authentication for Information Systems*, and DoDM5200.01v1_AFMAN 16-1404v1, *Air Force Information Security Program: Overview, Classification, and Declassification*. The PM documents cryptographic countermeasures in the Program Protection Plan. (T-1)**

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.

(Added)(DAF) This includes program information developed by DoD and non-DoD contractors in support of S&T efforts.

(Added)(DAF) A PPP documents how a program will protect critical information, components and critical program information. In addition to PPPs, Security Classification Guides also serve as the basis for protecting and building information security using DoDM 5200v2_AFMAN 16-1404v2, *Information Security Program: Marking of Information*. (T-0) Programs will work with the Original Classification Authority to determine the classification of prescribed elements of information and ensure adherence to classification marking requirements. (T-1) Classification by compilation, i.e., compilations of information that are individually unclassified (or classified at a lower level) may be classified or elevated in classification to a higher level if the compiled information reveals an association or relationship to a different classification level. This process will be used to determine distribution restrictions. Security classification guides also serve as the basis for protecting DAF data.

(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.

(Added)(DAF) Program information created by DoD and non-DoD contractors supporting S&T projects, experiments, and specific research should also be protected from compromise. (T-1)

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.

(c) (Added)(DAF) Contracting officers will use the Supplier Performance Risk System in their contracts to ensure compliance with Defense Federal Acquisition Regulation Supplement (DFARS) 204.73, *Safeguarding Covered Defense Information and Cyber Incident Reporting*. (T-0) This DFARS clause requires companies have summary results of their assessment of compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 revision 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* as required by DFARS 252.204-7019, *Notice of NIST SP 800-171 DoD Assessment* and DFARS clause 252.254-7012 if the offeror is required to implement NIST 800-171 for National Security System class determination.

(4) Software and Hardware.

(a) (Added)(DAF) Software vulnerabilities make up the majority of all system vulnerabilities. This calls for the use of DevSecOps in the integration of security at every phase of the software development lifecycle, from initial design through integration, testing, deployment, and software delivery. (T-1)

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).

(e) (Added)(DAF) Programs seeking additional cybersecurity, DevSecOps, supply chain, or weapon system resiliency information or support services should reference the following:

1. (Added)(DAF) Guidance for addressing software, hardware, and firmware protection measures can be found at the Joint Federated Assurance Center (JFAC) Portal [https://jfac.navy.mil/JFAC/]. JFAC is a federation to support trusted defense system needs and to ensure the security of software, firmware, and hardware developed, acquired, maintained, and used by the DoD.

2. (Added)(DAF) Supply chain risk management services are located on the DoD Supply Chain Risk Management (SCRM) [https://www.acq.osd.mil/dpap/pdi/cyber/enhanced_procedures_for_supply_chain_risk_management.html].

3. (Added)(DAF) Trusted Systems and Networks (TSN) strategies in accordance with DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted*

Systems and Networks (TSN) **shall also be incorporated. (T-0) Use Air Force and command focal points to initiate TSN activities and obtain supply chain threat documents.**

4. (Added)(DAF) DevSecOps and software factory services can be located on the Chief Software Officer website [https://software.af.mil].

5. (Added)(DAF) System security engineering and cyber resilience services are located on the Cyber Resilience Office for Weapon Systems (CROWS) website [https://www.my.af.mil/gcss-af/USAF/ep/globalTab.do?channelPageID=sE3494DD05DD7CCA3015DEBE7E0B50426].

(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.

(a) (Added)(DAF) Utilization of foreign owned and operated depot facilities outside the Continental United States present an increased national security challenge and risk to U.S. advanced technology and combat systems due to the overt foreign influence (depot ownership and labor force).

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.

(Added)(DAF) Acquisition Security is a key element of program protection for the planning and integration of all security disciplines and other defensive methods into the acquisition process. This protects weapon systems and related sensitive technology, technical data to include research data with military applications, and support systems

from foreign intelligence collection, unauthorized disclosure, sabotage, theft, damage throughout the system's life cycle.

(Added)(DAF) The use of automation continues to improve product development costs and reduce sustainment costs. These efforts are dependent on software to support automation. Software vulnerabilities make up the majority of all system vulnerabilities, thereby increasing the need to test using DevSecOps throughout the program lifecycle.

(Added)(DAF) S&T managers and engineering teams will also include acquisition/S&T security professionals with a broad understanding of security countermeasures, risk mitigation strategies, program and technology protection as part of their engineering team or Integrated Test Team to assist in developing technology and program protection strategies. (T-1)

a. Safeguard Information.

(Added)(DAF) Program Managers will be responsible for protecting their program information. (T-0) This requires program offices to follow guidance as outlined by the Chief Data Office throughout the program lifecycle to support acquisition security. By not identifying program and sharable information in security classification guides and data repositories for CUI, program protection efforts become more difficult. Contracting officers will use the Supplier Performance Risk System in their contracts to ensure compliance with Defense Federal Acquisition Regulation Supplement (DFARS) 204.73, *Safeguarding Covered Defense Information and Cyber Incident Reporting*. (T-0) DFARS clause 252.204-7012 requires companies to have summary results of their assessment of compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 revision 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, as required by DFARS 252.204-7019, *Notice of NIST SP 800-171 DoD Assessment Requirements* if the offeror is required to implement NIST 800-171 for National Security System class determination. (T-1)

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.

(8) (Added)(DAF) Program personnel will coordinate with local security office and report all actual or possible losses or compromises of classified information and CUI, in accordance with DoDM 5200.01v3_AFMAN 16-1404v3, *Information Security Program: Protection of Classified Information,* and AFGM 2021-16-01, *Air Force Guidance Memorandum for Controlled Unclassified Information (CUI)*. (T-0) Programs will also coordinate with the local security office and report as required on all possible (or actual) losses/compromises of classified information and/or as outlined in DoDI 5200.48, *Controlled Unclassified Information (CUI)*. (T-0)

(9) (Added)(DAF) The marking reference "For Official Use Only (FOUO)" is no longer valid. Any marking or reference to "FOUO" should be replaced with "CUI" if applicable. (T-0)

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.

(Added)(DAF) Program Managers shall establish support for acquisition security from intelligence and counterintelligence sources, and related system security in their technical risk management activities throughout the program lifecycle. (T-0)

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.

5. (Added)(DAF) Physical and information security based on the required design and performance characteristics of the system architecture.

6. (Added)(DAF) ***Department of the Air Force United States Air Force System Security Engineering Cyber Guidebook*** **for guidance.**

(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.

(f) (Added)(DAF) Digital engineering, DevSecOps, MOSA, and interoperability will be considered and implemented into the program lifecycle to the greatest extent possible. (T-1)

(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.

1. (Added)(DAF) At a minimum, DoD Information Network and external interfaces shall implement FIPS 140-3, *Security Requirements for Cryptographic Modules,* standards. (T-0)

(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.

(a) (Added)(DAF) Programs will refer to the Department of the *Air Force System Security Engineering Cyber Guidebook* for guidance, and programs will also develop program data requirements during this process. (T-1) (Added)(DAF) The lead systems engineer will review the PPP for currency at each decision point or annually at a minimum. (T-1) Critical Program Information and critical components throughout the life cycle of the program and at each milestone should also be verified. (T-1) Sustainment programs, whether or not undergoing modifications, should follow the same process to review Critical Program Information (CPI) and critical components and then update their PPP. (T-0)

(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.

(c) (Added)(DAF) Refer to the Department of the *Air Force System Security Engineering Cyber Guidebook* for guidance. (T-1)

(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.

(a) (Added)(DAF) Intelligence and counterintelligence professionals will provide the applicable threat information. (T-1)

(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.

1. (Added)(DAF) Program specific guidance can be developed during and after identification of critical program information and critical technology elements.

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

1. (Added)(DAF) Programs will use trusted and assured DoD microelectronics suppliers and practices to the greatest extent possible. (T-1). (Added)(DAF) This guidance can be developed during and after identification of critical program required to be protected through anti-tamper measures.

(c) (Added)(DAF) Apply DoD Executive Agent for AT guidance (e.g., the AT Technical Implementation Guide) to determine requirements for planning, designing, implementing AT and exportability features, as appropriate, to technology and systems when outside of U.S. control. (T-0)

(d) (Added)(DAF) SAF/AQL serves as the DAF Office of Primary Responsibility for AT. Submit AT Plans to SAF/AQLA for review and coordination before Milestones A, B, and C. This includes AT Plans for domestic programs, as well as those for Foreign Military Sales and Direct Commercial Sales. (T-1)

(e) (Added)(DAF) Coordinate with SAF/AQLA for programs where AT protections are not required. (T-1)

(7) (Added)(DAF) Programs will use Trusted Systems and Networks (TSN) strategies in accordance with DoDI 5200.44 along with SCRM and intelligence data available. (T-1) 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.

1 (Added)(DAF) Use programming languages that can be evaluated; these will be used with a combination of integrated testing methods like statistical analysis, object and source code analysis, dynamic and fuzz testing, and penetration testing to identify and mitigate vulnerabilities to support a continuous accreditation process. (T-1)

2 (Added)(DAF) Refer to DAFI 63-101/20-101; DAFI 63-150_DoDI 5000.87, *Operation of the Software Acquisition* Pathway; DAFMAN 63-128, *Integrated Life Cycle Management;* and the JFAC Portal (https://jfac.navy.mil/JFAC/) for software assurance resources, best practices, and guidance.

(b) Hardware assurance.

1. (Added)(DAF) Refer to the JFAC Portal (https://jfac.navy.mil/JFAC/) for hardware assurance resources, best practices and guidance.

(c) Procurement strategies.

(d) Anti-counterfeit practices.

(e) (Added)(DAF) Firmware assurance. The Program Manager implements and applies firmware assurance for system critical components to increase the level of confidence that the firmware functions as intended and is free from design vulnerabilities, either intentionally or unintentionally inserted.

(f) (Added)(DAF) SCRM.

(g) (Added)(DAF) Utilization of intelligence data.

(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.

(a) (Added)(DAF) This will be done in coordination with the local security, counterintelligence, and intelligence resource offices. (T-1)

(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.

(e) (Added)(DAF) Programs will refer to the *Department of the Air Force System Security Engineering Cyber Guidebook* (Appendices C and D) for guidance. (T-1)

(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. **(Added)(DAF) Monitoring includes determining AT impacts as a result of changes to CPI, addresses threats and major AT vulnerabilities, and identifying and reporting tamper events.**

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.

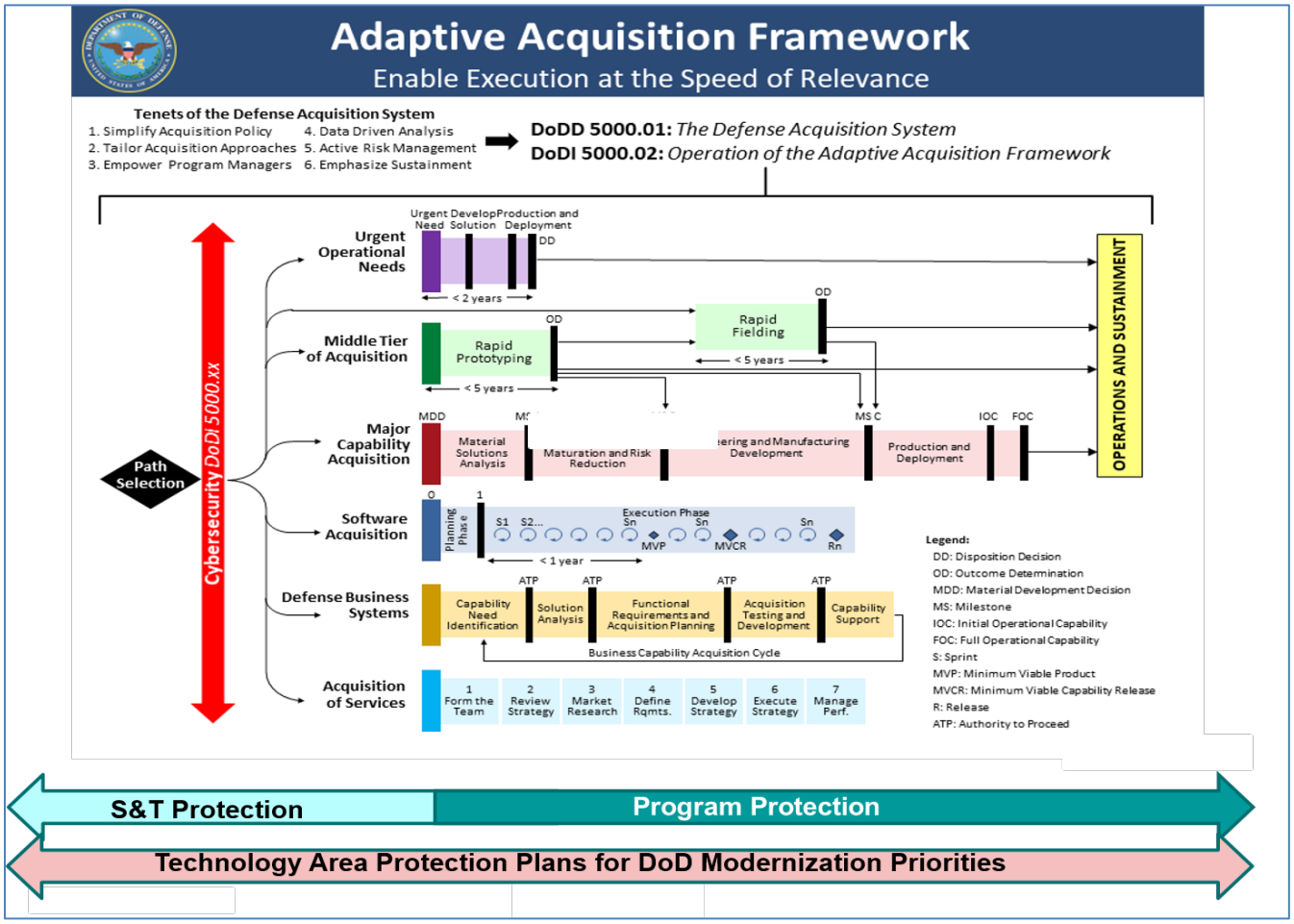
(4) Procurement actions.

(5) (Added)(DAF) Team composition. Include acquisition/S&T/engineering security personnel with a broad understanding of security countermeasures, risk mitigation strategies, program and technology protection as part of their engineering team or Integrated Test Team to assist in developing and monitoring program protection strategies. Acquisition security personnel will also engage with counterintelligence and intelligence resources. (T-0)

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 **(Added)(DAF) and intelligence efforts.**

(6) Law enforcement activities.

(7) (Added)(DAF) Protection of critical program information. Technology areas need security classification guides to identify critical program information. If none exists, decision authorities and Program Managers will create a security classification guide for their technology area that specifies the type and protection requirements, but that are not in conflict with existing security classification guides. (T-1) In the interim, use the Cybersecurity Classification/Declassification Guide for Air Force Weapon Systems until technology areas finalize their classification guide. (T-1)

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.

(Added)(DAF) DAF PPP will also address Critical Program Information, Criticality Analysis, Risk Assessment, Horizontal Protection, the acquisition security database unless waived by DA. (T-0)

(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.

(d) (Added)(DAF) Additional PPP content. The PM documents the following in the PPP:

1. (Added)(DAF) How the program addresses system security engineering requirements in systems engineering technical reviews, functional and physical configuration audits, and change analyses. Program Managers document program protection-oriented entry and exit criteria for engineering and technical reviews in the Program Protection Plan. The PM ensures that program protection requirements are thoroughly analyzed prior to design and implementation, and assessed as part of the test and evaluation strategy. (T-1)

2. (Added(DAF) How program protection requirements and considerations are managed during sustainment.

3. (Added(DAF) How program personnel and contractors report and respond (procedures) to attempted or successful Critical Program Information compromises, supply chain exploitations, counterfeit infiltration, and the compromise of controlled unclassified information or classified information. The PM manages risk to Controlled Unclassified Information consistent with DoDI 5200.48, DoDI 5230.24, *Distribution Statements on Technical Documents*, and DoDI 8582.01, *Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information*.

4. (Added)(DAF) Other System Security-Related Plans and Documents. The PM records security relevant program documents (e.g., plans, strategies, standards, analysis results, letters of agreement or memoranda of understanding associated with foreign sales or usage), their originating organization, location, and points of contact. (T-1)

(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. (Added)(DAF) Refer to the *Department of the Air Force System Security Engineering Cyber Guidebook* for guidance on cybersecurity and cyber resilient engineering). (T-1)

(c) (Added)(DAF) For all programs where the DAE is not the MDA the respective AF or SF MDA will be the approval authority, SAF/AQR will review and coordinate PPPs for ACAT I programs. (T-1)

(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.

(4) (Added)(DAF) Program Managers will upload their Program Protection Plans for all Major Defense Acquisition Programs (MDAP) in the Acquisition Information Repository (AIR). (T-1)

(5) (Added)(DAF) Programs identified on the DoD Critical Program and Technology List will review and update PPPs annually. (T-1)

(6) (Added)(DAF) Trusted Systems and Networks Focal Point. The HAF Trusted Systems and Networks focal point is the overall AF Trusted Systems and Networks lead, performs those duties that cannot be performed at the MAJCOM level, and resolves disputes between implementing commands on matters concerning Enterprise-level Trusted Systems and Networks activities. The HAF Trusted Systems and Networks focal point is SAF/AQR.

(a) (Added)(DAF) Implementing commands should each designate a Trusted Systems and Networks focal point to perform the following activities: (T-1)

1. (Added)(DAF) Coordinate MAJCOM requests for threat analysis of suppliers of critical components.

2. (Added(DAF) Coordinate use of Trusted Systems and Networks resources, including Subject matter experts and tools.

3. (Added)(DAF) Coordinate with the HAF focal point in the development of Trusted Systems and Networks requirements, best practices, and mitigations.

4. (Added)(DAF) Monitor the identification of mission critical functions and critical components as well as Trusted Systems and Networks planning and implementation activities documented in the Program Protection Plan.

(b) (Added)(DAF) The PM coordinates with the implementing command's Trusted Systems and Networks focal point regarding Trusted Systems and Networks threat identification, best practices, processes, techniques and procurement tools. The PM will complete TSN analysis by conducting criticality analysis, threat assessment, vulnerability assessment, risk assessment, and selection of appropriate protective measures for the mission critical functions and critical components. (T-0)

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.

(3) (Added)(DAF) Test and Evaluation Master Plan guidance can be found in DoDI 5000.89, *Test and Evaluation,* and DAFI 99-103_DoDI 5000.89, *Capabilities-Based Test and Evaluation*.

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
(Added)(DAF) AF/A8	**Deputy Chief of Staff for Plans and Programs**
(Added)(DAF) AFPAM	**Air Forec pamphlet**
(Added)(DAF) AF/TE	**Director Air Force Test and Evaluation**
(Added)(DAF) AIR	**acquisition information repository**
AT	anti-tamper
BA	budget activity
(Added)(DAF) CAE	**Component Acquisition Executiv**
(Added)(DAF) CFIUS	**Committee for Foreign Investment in the United States**
Added)(DAF) CFR	**Code of Federal Regulations**
(Added)(DAF) CPI	**critical program information**
(Added)(DAF) CROWS	**Cyber Resiliency Office for Weapon Systems**
CTI	controlled technical information
CUI	controlled unclassified information
(Added)(DAF) DA	**decision authority**
DAE	defense acquisition executive
DAS	Defense Acquisition System
(Added)(DAF) DevSecOps	**Development, Security, and Operations**
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DoDD	DoD directive
DoDI	DoD instruction
(Added)(DAF) DPAS	**Defense Priorities and Allocation Systems**
(Added)(DAF) FAR	**Federal Acquisition Regulation**
FFRDC	federally funded research and development center
JCIDS	Joint Capability Integration and Development System
JFAC	Joint Federated Assurance Center
(Added)(DAF) MOSA	**modular open systems approach**
(Added)(DAF) NIST	**National Institute of Standards and Technology**

ACRONYM	MEANING
PPP	program protection plan
S&T	science and technology
(Added)(DAF) SAF/AA	**Administrative Assistant Secretary to the Secretary of the Air Force**
(Added)(DAF) SAF/AQ	**Assistant Secretary of the Air Force for Acquisition, Technology and Logistics**
(Added)(DAF) SAF/AQR	**Assistant Secretary for Science, Technology and Engineering**
(Added)(DAF) SAF/AQX	**Deputy Assistant Secretary for Acquisition Integration**
(Added)(DAF) SAE	**Service Acquisition Executive**
(Added)(DAF) SAF/CN	**Chief Information Officer**
(Added)(DAF) SAF/CO	**Chief Data Officer**
(Added)(DAF) SAF/CSwO	**Chief Software Office**
(Added)(DAF) SAF/FM	**Assistant Secretary of the Air Force for Financial Management**
(Added)(DAF) SAF/SQ	**Assistant Secretary of the Air Force Space Acquisition and Integration**
SCRM	supply chain risk management
(Added(DAF) SF/TE	**Space Force Test and Evaluation**
(Added)(DAF) SPPBE	**Strategy, Planning, Programming, Budgeting, and Execution**
(Added)(DAF) STINFO	**Scientific and Technical Information**
TAPP	technology area protection plan
(Added)(DAF) USAF	**United States Air Force**
(Added)(DAF) USC	**United States Code**
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(R&E)	Under Secretary of Defense for Research and Engineering
(Added)(DAF) USSF	**United States Space Force**

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
(Added)(DAF) acquisition security	**Acquisition Security is a key element of program protection for the planning and integration of all security disciplines and other defensive methods into the acquisition process. Acquisition security seeks to protect weapons systems and related sensitive technology, technical data to include research data with military applications, and support systems from foreign intelligence collection, unauthorized disclosure, sabotage, theft, or damage throughout a system's life cycle.**

TERM	DEFINITION
horizontal protection	Defined in DoDI 5200.39
(Added)(DAF) Supply Chain Risk Management	**The systematic process for managing risk by identifying, assessing, and mitigating actual or potential threats, vulnerabilities, and disruptions to the AF supply chain from beginning to end to ensure mission effectiveness.**

REFERENCES

(Added)(DAF) 15 CFR 700, Defense Priorities and Allocation System

(Added)(DAF) 50 USC, *War and National Defense*, Section 2061

Defense Federal Acquisition Regulation Supplement, current edition

(Added)(DAF) Directive-type Memorandum DTM 15-002, *Policy Guidance for the Processing of National Interest Determinations (NIDWS) in Connection with Foreign Ownership, Control, or Influence (FOCI)*, February 11, 2015, as amended

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

(Added)(DAF) DoD Directive 3150.02, "*DoD Nuclear Weapons Surety Program*," August 31, 2018

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

(Added)(DAF) DoDI 2000.25, *DoD Procedures for Reviewing and Monitoring Transactions Filed with the Committee on Foreign Investment in the United States (CFIUS)*, December 16, 2021

(Added)(DAF) DoD Instruction, 2010.06, "*Materiel Interoperability and Standardization with Allies and Coalition Partners,"* August 31, 2018

(Added)(DAF) DoD 4400.01-M, "*Priorities and Allocation Manual*," February 2, 2002

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

(Added)(DAF) Executive Order 13526, "*Classified National Security Information*," December 29, 2009

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

(Added)(DAF) DoDM 5030.55_AFMAN63-103, *DoD Procedures for Joint DoD-Department of Energy/National Nuclear Security Administration (DOE/NNSA) Nuclear Weapon Life-Cycle Activities*, August 10, 2018

(Added)(DAF) DoDM5200.01v1_AFMAN 16-1404v1, *Air Force Information Security Program: Overview, Classification, and Declassification*, January 11, 2021

(Added)(DAF) DoDM 5200.01v2_AFMAN 16-1404v2, *Information Security Program: Marking of Classified Information*, January 7, 2021

(Added)(DAF) DoDM 5200.01v3_AFMAN 16-1404v3, *Information Security Program: Protection of Classified Information*, December 23, 2020

(Added)(DAF) AFPD 63-1/20-1, *Integrated Life Cycle Management*, August 7, 2018

(Added)(DAF) AFPD 90-6, *Air Force Strategy, Planning, Programming, Budgeting, and Execution (SPPBE) Process*, June 26, 2019

(Added)(DAF) AFMAN 16-101, *Security Cooperation (SC) and Security Assistance (SA) Management*, August 2, 2018

(Added)(DAF) DAFMAN 16-201, *Department of the Air Force Foreign Disclosure and Technology Transfer Program*, January 19, 2021

(Added)(DAF) AFI 33-322, *Records Management and Information Governance Program*, March 23, 2020

(Added)(DAF) DAFI 33-360, *Publications and Forms Management*, December 1, 2015

(Added)(DAF) DAFI 61-201, *Management of Scientific and Technical Information (STINFO)*, November 30, 2020

(Added)(DAF) AFI 63-101/20-101, *Integrated Life Cycle Management*, June 30, 2020

(Added)(DAF) DAFI 63-150_DoDI 5000.87, *Operation of the Software Acquisition Pathway*, August 11, 2021

(Added)(DAF) AFI 65-508, *Cost Analysis Guidance and Procedures*, December 6, 2018

(Added)(DAF) DAFMAN 65-605, *Budget Guidance and Technical Procedures, Volume 1,* March 31, 2021

(Added)(DAF) AFI 16-701, *Management, Administration and Oversight of Special Access Programs*, February 18, 2014

(Added)(DAF) AFI 91-101, *Air Force Nuclear Weapons Surety Program*, March 26, 2020

(Added)(DAF) DAFI 99-103_DoDI 5000.89, *Capabilities-Based Test and Evaluation*, December 9, 2021

(Added)(DAF) AFGM 2021-16-01, *Air Force Guidance Memorandum for Controlled Unclassified Information (CUI)*, July 22, 2021

(Added)(DAF) *Cybersecurity Classification/Declassification Guide for Air Force Weapon Systems*, April 17, 2017

(Added)(DAF) *Department of the Air Force System Security Engineering Cyber Guidebook*, version 4.0, July 26, 2021

(Added)(DAF) DAFMAN 63-128, *Integrated Life Cycle Management*, February 3, 2021

(Added)(DAF) DFARS 204.73, *Safeguarding Covered Defense Information and Cyber Incident Reporting*

(Added)(DAF) NIST SP 800-171 revision 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, February 2021

(Added)(DAF) FIPS 140-3, *Security Requirements for Cryptographic Modules,* 22 March 2019

(Added)(DAF) Prescribed Forms: None

(Added)(DAF) Adopted Forms:

(Added)(DAF) AF Form 847, *Recommendation for Change of Publication*

(Added)(DAF) BIS-999, ***Request for Special Priorities Assistance***

(Added)(DAF) DD Form 691, ***Application for Priority Rating for Production or Construction Equipment***