DoD Instruction 5000.90

Cybersecurity for Acquisition Decision Authorities and Program Managers

Originating Component:	Office of the Under Secretary of Defense for Acquisition and Sustainment
Effective:	December 31, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Incorporates and Cancels:	See Paragraph 1.3.
Approved by:	Ellen M. Lord, Under Secretary of Defense for Acquisition and Sustainment

Purpose: In accordance with the authority in DoD Directive (DoDD) 5135.02, this issuance establishes policy, assigns responsibilities, and prescribes procedures for the management of cybersecurity risk by program decision authorities and program managers (PMs) in the DoD acquisition processes, compliant with the requirements of DoDD 5000.01, DoD Instruction (DoDI) 5000.02T, DoDI 8510.01, and Chairman of the Joint Chiefs of Staff Instruction 5123.01H.

TABLE OF CONTENTS

TABLES

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

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 the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

1.2. POLICY.

Cybersecurity:

a. Is foundational to the Defense Acquisition System (DAS) and an intrinsic program manager (PM) responsibility when a program uses any acquisition pathway of the Adaptive Acquisition Framework (AAF) as described in DoDI 5000.02.

b. Controls are a targeted response to specific cybersecurity threats identified in the program's Validated Online Lifecycle Threat (VOLT), or equivalent threat assessment.

c. Planning and implementation requires specific changes to program engineering and supply chain risk management (SCRM) processes.

d. Leaders and experts must address how cybersecurity will evolve as technology and threats advance for a program's lifecycle.

1.3. SUMMARY OF INCORPORATION AND CANCELLATION.

Incorporates and cancels Enclosure 13 of DoDI 5000.02T.

SECTION 2: RESPONSIBILITIES

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

In addition to the responsibilities in Paragraph 2.6., the USD(A&S):

a. Establishes policy and provides guidance to establish the accountability and responsibilities of the acquisition milestone decision authorities (MDA), other decision authorities (DA) and PMs for ensuring that cybersecurity risks are properly assessed and managed within the AAF in consultation with the DoD Chief Information Officer (CIO); Commander, United States Cyber Command (CDRUSCYBERCOM); Chairman of the Joint Chiefs of Staff; and the Under Secretary of Defense for Intelligence and Security (USD(I&S)).

b. Establishes policy, standards, and guidance, in coordination with the DoD CIO and USD(I&S), to qualify, quantify, and illuminate cybersecurity risks to acquisition programs arising from adversaries targeting suppliers and supply chains.

c. Establishes policy, in coordination with the USD(R&E), to identify:

(1) Operational effectiveness of systems, and

(2) Procurement, supply chain, industrial base, scalability, and fielding inputs that inform investments to ensure the sustainment of a system throughout its lifecycle.

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

In the context of the AAF in supporting the responsibilities in Paragraph 2.6., the USD(R&E):

a. Provides DoD-wide policy framework and direction for technical and engineering protections to manage the risks to programs and systems from hardware, software, cyber and supply chain vulnerabilities, and reverse engineering.

b. Establishes and maintains policy, guidance, and training for technology area protection plans and program protection plans.

c. Leads Defense Damage Assessment Management Office under the Strategic Technology Protection and Exploitation Maintaining Technology Advantage directorate within USD(R&E) to understand how cyber incidents affect the Defense Industrial Base (DIB).

2.3. DOD CIO.

In addition to the responsibilities in Paragraph 2.6., the DoD CIO:

a. Maintains:

(1) The DoD cybersecurity policies that establish the processes and standards used by programs who produce information technology (IT) systems.

(2) The guidance, standards, and tools that support DoD cybersecurity policies.

(3) The Risk Management Framework Knowledge Service, made available to the DoD Components, containing cybersecurity risk management requirements, implementations, assessments, and monitoring documents at https://rmfks.osd.mil/login.htm.

b. Advises the USD(A&S):

(1) On interpreting and implementing cybersecurity policies and associated guidance, standards, and tools that support the AAF.

(2) On cybersecurity risk management implications of proposed and changing AAF policies and guidance.

c. In accordance with DoDI 5000.UH, reviews and approves the cybersecurity strategy for all Acquisition Category ID programs containing IT, including National Security Systems, before the MDA/DA makes milestone decisions or contract awards.

d. Coordinates with the USD(A&S) on:

(1) Interoperability requirements development.

(2) Interoperability test and certification.

(3) Prerequisites for connection of IT.

(4) Oversight of IT interoperability, in coordination with the DoD Components and other mission partners.

e. Appoints a Senior Information Security Officer (DoD SISO) pursuant to Section 3554 of Title 44, United States Code (U.S.C.) and in accordance with DoDI 8500.01.

f. For suppliers or products requiring action pursuant to Section 2339a of Title 10, U.S.C., and in coordination with the USD(I&S) and USD(A&S), prepares and executes an action package that contains the joint recommendation of the DoD CIO and USD(A&S), on the basis of a risk assessment by the USD(I&S), that there is a significant supply chain risk to a national security system as defined in Section 3542(b) of Title 44, U.S.C.

2.4. CDRUSCYBERCOM.

In addition to the responsibilities in Paragraph 2.6., CDRUSCYBERCOM advises the USD(A&S) on:

a. Implications of cybersecurity vulnerabilities found in materiel cyber solutions and the feasibility of cyber operations as a mitigation strategy for those vulnerabilities.

b. Techniques, technologies, and standards that can be incorporated into materiel cyber solutions to improve the ability of United States Cyber Command forces to defend systems employing those solutions during conflict.

c. Orders issued by CDRUSCYBERCOM (via DoD Components) for fielded systems, infrastructure, and programs that are designed to close high-priority vulnerabilities or mitigate adversary tactics, techniques, and procedures in a time-sensitive environment.

2.5. USD(I&S).

In addition to the responsibilities in Paragraph 2.6., the USD(I&S):

a. Establishes policies, program planning and execution, or use of resources for the protection of classified information and controlled unclassified information (CUI).

b. Advises the USD(A&S) and AAF PM on the incorporation of Intelligence Community products, especially cyber threat assessments, into the AAF.

c. Provides a cyber threat assessment capability for DoD Components that is optimized for effectively driving risk-appropriate cybersecurity within the AAF.

d. Authorizes and directs the Director, Defense Intelligence Agency (DIA) to:

(1) Manage the Defense Intelligence Threat Library cyber threat modules.

(2) Assess cyber vulnerabilities and perform the validation of VOLTs for Acquisition Category ID and IAM acquisitions.

2.6. DOD AND OSD COMPONENT HEADS.

Through the delegated MDA/ Decision Authorities (DAs) of the Component acquisition executives and the PMs for individual acquisition programs of any size (i.e., acquisition category), the DoD and OSD Component heads oversee the administration of cybersecurity in AAF programs.

a. MDA/DAs:

(1) Are responsible for appropriately and effectively applying the requirements of this issuance in each program that they oversee.

(2) Ensure that PMs assess, mitigate, and monitor cybersecurity risks to the:

(a) Program information and the information system (IS); and

(b) Platform information technology (PIT) being acquired by the program.

(3) Ensure that the cybersecurity plans and results produced by PMs are in accordance with this issuance, including the requirement for Cybersecurity Strategies for all critical and mission essential systems containing IT. Component-required procedures will not supersede the requirements for acquisition programs stated in this issuance.

b. PMs are responsible for the cybersecurity of their programs, systems, and information, as assisted by supporting organizations. PMs:

(1) Are responsible for cybersecurity from the earliest exploratory phase and throughout all stages of the acquisition to include the following activities:

(a) System concept trades.

(b) Design.

(c) Development.

(d) Test and evaluation (T&E).

(e) Production.

(f) Fielding.

(g) Sustainment.

(h) Disposal.

(2) Must identify:

(a) Risks, including financial, schedule, functional, supply chain, and cybersecurity.

(b) The consequences of a cybersecurity breach, including situations where a cybersecurity breach or failure would jeopardize military technological advantage or mission-critical functionality. These potential breaches and their consequences must be documented in the Cyber Security Strategy annex to the Program Protection Plan. Potential breaches include failures in any of the following:

1. The IS or PIT hardware and software being acquired by the program.

2. Program information.

3. Organizations and personnel.

4. Enabling networks.

5. Systems, enabling systems, and supporting systems.

6. Supply chain security.

(3) In accordance with DoDI 5000.02T, must ensure that their Program Management Office includes and decomposes cybersecurity requirements throughout the acquisition lifecycle: from needed security capabilities, to operational requirements for security, to system and technical requirements, to specifications as implemented controls.

2.7. VICE CHAIRMAN OF THE JOINT CHIEFS OF STAFF.

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

a. Consults with the USD(A&S), as appropriate, on the joint force warfighting implications of USD(A&S) policies and guidance for cybersecurity risk management in the AAF.

b. Provides advice to the DoD Components on:

(1) Operational cybersecurity interoperability across the joint force.

(2) Cybersecurity interoperability of military networks.

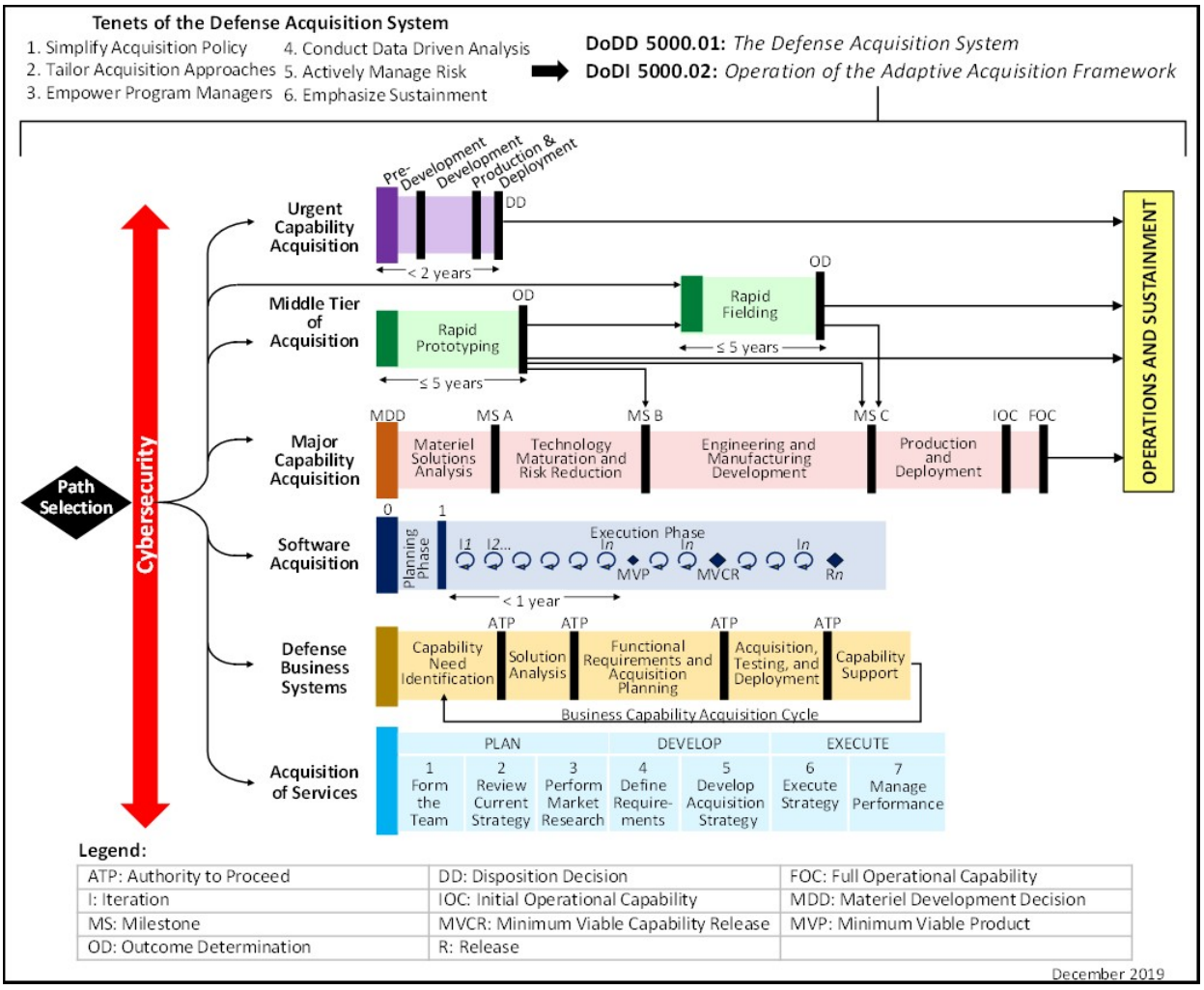
(3) Alignment with future United States Cyber Command cyberspace warfighting concepts and architectures.

SECTION 3: PROCEDURES

3.1. CYBERSECURTIY FOUNDATIONS IN THE DEFENSE ACQUISITION SYSTEM (DAS).

In order to harden the U.S.'s weapon systems and infrastructure, the Department must inculcate cyber security into all aspects of the DAS and operations. The focus on cybersecurity must encompass platforms, weapons, and the DIB and must be regularly assessed, properly resourced, and continually mitigated. Cybersecurity crosses all pathways within the AAF.

Figure 1. AAF



a. The DAS ensures that the DoD is equipped to win military operations against all adversaries in all warfighting domains—including cyberspace. This is especially important when the warfighting domains are actively and aggressively contested.

b. Cyber vulnerabilities provide opportunities for adversaries to exploit, steal, alter, interrupt, or destroy system functionality, information, or technology.

c. Program cybersecurity must mitigate cyber vulnerabilities to protect:

(1) Operational effectiveness of the system (i.e., system functions, mission execution, system performance, and system resilience).

(2) System program information that adversaries might use to develop attacks against the system functions.

d. PMs must reinforce cybersecurity against:

(1) Known and anticipated threats—identified during the preliminary stages of development.

(2) Potential future vulnerabilities —identified through threat monitoring and mitigated by designing systems to rapidly address cyber risks by using modular open systems architectures.

e. PMs must deploy cybersecurity risk analyses and controls mapping early in the system development to prevent loss of programmatic and operational hardware, software, and data throughout the remainder of the lifecycle.

f. Cybersecurity as a foundational requirement is:

(1) Represented within the system survivability key performance parameters as a mandatory capability consideration in all DoD acquisitions.

(2) Continuously enforced through the risk management framework (RMF) and SCRM systems described in Paragraphs 3.3 and 3.4.

g. Cybersecurity considerations must be addressed:

(1) In all acquisition programs using any of the acquisition pathways of the AAF.

(2) At all classification levels (including UNCLASSIFIED).

(3) Throughout the entire acquisition and sustainment life cycle.

3.2. CYBERSECURITY DRIVEN BY THREAT.

PMs will incorporate cybersecurity requirements and apply controls to mitigate observed, anticipated, or emerging threats so that DoD systems are effective in cyber-contested operational environments. Designs and architectures must address technology and cyber threat evolution to maintain mission effectiveness beyond the near term.

a. System Threat Analysis.

(1) PMs must use cyber threat information produced by the Intelligence Community in development of their cyber security strategy and assessment of risk. Intelligence Community products that specifically support acquisition programs include, but are not limited to:

(a) Threat modules.

(b)Validated online lifecycle threat reports.

(c) Technology targeting risk assessments.

(2) PMs will consult with intelligence and security credentialed professionals to obtain cyber threat and security inputs to the program and RMF processes.

(3) Every program that requires an authority to operate (ATO) in accordance with DoDI 8510.01 will conduct an assessment of program impacts from cyber threats to drive their efforts leading to an ATO.

b. Threat Mitigation linked to ATO.

(1) In accordance with DoDI 8510.01, IT and PIT systems will update their ATO at least every 3 years depending on risk.

(2) Before a program receives an ATO, the PM will review the program's most recent threat assessment of the system's cyber-vulnerabilities that must have been issued by the Intelligence Community within the 12 months before issuance of the ATO.

c. Continuous Cyber Threat Analysis.

(1) Throughout the acquisition lifecycle of any acquisition pathway, the PM must maintain awareness of threat actor activities that could impact the platform, enterprise, or mission.

(2) If a new, or previously unaddressed, threat emerges as a possible risk to the system, the PM will initiate a risk assessment to identify the risk to the platform. Based upon the changes and this platform risk assessment, Authorizing officials (AOs), in conjunction with the affected commander(s) or director(s), should then conduct an operational risk assessment to identify the risk to the enterprise, and mission. The DoD CIO, in conjunction with the Office of the Chief Information Security Officer for Acquisition, may reassess the risk posture of the system.

(3) The system's Cyber Survivability Risk Posture could help provide an easier-to-digest view of whether a program had already planned for the emergent threat and related or supported missions.

(4) In addition to allocating resources to constantly improve software, manufacturing, reliability, and trustworthiness throughout a program's lifecycle, PMs will dedicate resources and personnel to continually assess and mitigate a program's cyber risk.

d. Tailoring.

(1) The cybersecurity ATO is a requirement for systems in operational use that certifies that the cybersecurity controls incorporated into the IS or PIT enable it to be effective in the anticipated cyber-contested environment.

(2) In accordance with DoDI 8510.01, the ATO is issued by an AO based on the technical findings of a security controls assessor.

(3) The PM, with concurrence from the AO and DA, can tailor the RMF process to achieve an ATO commensurate with the cyber risk of the program.

3.3. CYBERSECURITY PLANNING AND EXECUTION.

a. Planning Cybersecurity Activities.

(1) The PM is responsible for ensuring that the cybersecurity requirements are considered in all aspects of their program to include operational cybersecurity and supply chain resilience.

(2) The PM is expected to delegate responsibility to members of the program staff with technical knowledge of cybersecurity to produce the Cybersecurity Strategy Annex of the Program Protection Plan in accordance with DoDI 5000.02T. The cybersecurity annex will document how the system will operate in a cyber-contested environment. For platform and weapon systems that require an ATO in accordance with DoDI 8510.01, the cybersecurity annex will document the following:

(a) A plan of action and milestones (POA&M) to address known vulnerabilities.

(b) Implementation of continuous monitoring of risk based on cyber threats, vulnerabilities, and mitigations.

(c) Implementation of the RMF process within the program management office's acquisition and engineering processes for development, procurement, testing, and sustainment.

(d) The need for operational cyber resilience and, if appropriate, the resulting monitoring, responding, and recovering of the system and mitigation of the vulnerabilities.

b. Executing Cybersecurity Throughout the Acquisition Lifecycle.

(1) PMs will allocate the resources and personnel required to mitigate cyber risk throughout the lifecycle of the program.

(2) PMs should conduct periodic threat-representative adversarial assessments to assess the ability of the cyber technologies in the materiel solution to complete missions in a cyber-contested environment.

(3) If an ATO is required, identify the AO responsible and ensure the AO is informed on cyber risks, threats, and associated mitigations for the program to operate in a threat-informed, cyber-contested environment.

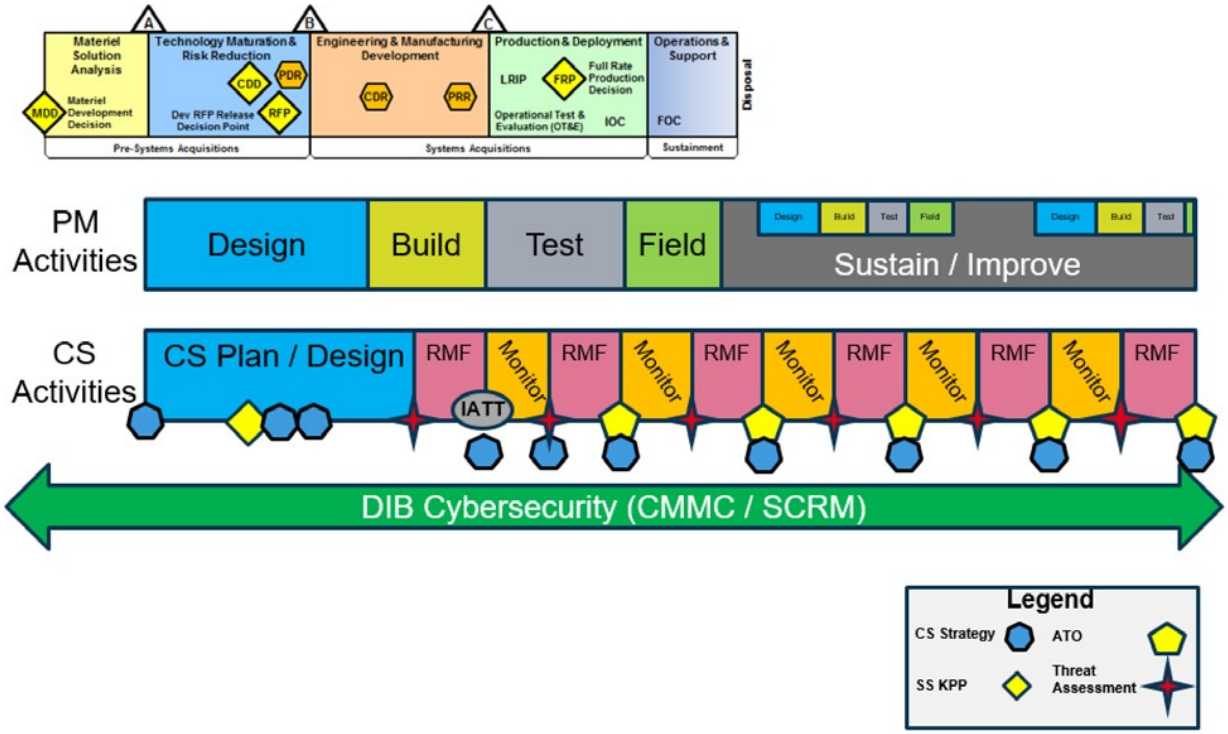
(4) Figure 2 represents the implementation of threat-based cybersecurity throughout the Acquisition Lifecycle. While this figure depicts the Major Capability Acquisition pathway, the concepts apply to all pathways. In essence, PMs must design, build, test, field, and sustain their product. Likewise, PMs have associated cybersecurity activities they must accomplish. This starts with the PM's cybersecurity strategy and continues through the RMF process leading to an ATO.

(5) PMs, in coordination with AOs, must revisit a program's cybersecurity posture based on threat assessments and continuous monitoring. Each iteration should conclude with the AO validating the PM's cybersecurity strategy and updated POA&M in accordance with Figure 2.

(a) While the AO may authorize a continuous ATO (cATO), a cATO is only appropriate for products that have a robust automated monitoring capability that allows real or close to real time situational awareness of their cybersecurity status. At this time, a cATO may only be appropriate for programs in the Software and Defense Business System pathways and not for software-enabled hardware programs.

(b) The iterative ATO process depicted in Figure 2 enables AOs to monitor risks codified in security assessment reports and progress against the program's cybersecurity strategy and cybersecurity POA&Ms, all based on threat assessments from the Intelligence Community.

Figure 2. Cybersecurity Planning and Execution



c. Resourcing Cybersecurity Activities.

In addition to allocating and protecting resources to constantly improve software, manufacturing, and reliability throughout a program's lifecycle, the PM will also dedicate program resources and personnel to continually assess and mitigate the program's cybersecurity risk by monitoring:

(1) New techniques and technologies for potential inclusion in the system baseline to improve its abilities to protect, detect, and recover from attacks.

(2) The emergence of exploitable cyber vulnerabilities.

(3) Methods to eliminate or mitigate vulnerabilities in accordance with DoD CIO guidance regarding vulnerability management.

(4) The threat environments where the system is, or is to be, deployed to determine if there are major changes that require updates to the system's cybersecurity controls.

3.4. CYBERSECURITY IN THE SUPPLY CHAIN.

Over the past decade, the United States' strategic competitors have been able to exploit vulnerabilities in the DoD supply chain by stealing U.S. intellectual property and decreasing confidence in the security of products delivered to the DoD. Contractor facilities—including design, development, and production environments, networks, supply chains, and personnel—can be used by threat actors as cyber pathways to access government program organizations or fielded systems to steal, alter, or destroy system functionality, information, or technology. The DoD must deliberately harden the supply chain commensurate with the risk to national security. For SCRM:

a. PMs will conduct SCRM, to include Cyber-SCRM. This includes, at a minimum, conducting market research to assess potential vendors to determine if they:

(1) Provide products and components, or sub-components, sourced through original equipment manufacturers or authorized resellers.

(2) Have previously incurred significant malicious network intrusions, data breaches, loss of client data, or intellectual property.

(3) Have obtained a CMMC certification level indicating that they practice, at least, basic cyber hygiene (e.g., access management, timely patch management, identity management, and password management).

b. The PMs will consider maintaining a visualization (illumination) of the supply chain in order to have situational awareness of the risks and vulnerabilities throughout the program's supply chain, especially those on the USD(R&E) Critical Technology List.

c. PMs will:

(1) Consider the source of products that may be supplied to fulfill program requirements, and seek alternatives to design of performance specifications or other program requirements that may necessitate the use of sources owned by, controlled by, or subject to the jurisdiction of a foreign adversary's government. The program PM will maintain a complete list that shows, to the furthest extent possible:

(a) The ownership of commercial companies that currently do, or potentially will, supply (hardware, software, or firmware) components to the program, and therefore may be subject to influence or control by threat actors with a known interest in the IS or PIT being acquired by the program.

(b) Technology relationships with other companies that are known to already be under the influence or control of threat actors.

(2) Take action to manage supply chain risks, including those associated with foreign ownership, control, or influence concerns, commensurate with the risk tolerance level of the system or mission in question.

(3) Counter risks to and from a product by applying a framework for cybersecurity SCRM due diligence, that links supply chain risk tolerance with the importance of the systems purchased (see Table 2).

Table 1. SCRM Actions by Risk Tolerance Level

High Risk Tolerance	High risk tolerance applies to simplified procurements, like computers at the Defense Commissary Agency. PMs should: • Exercise caution regarding products originating from sources with identified foreign ownership, control, or influence concerns. • Utilize approved products lists. • Maintain assurance through industry standards. • Balance risk against mission type.
Moderate Risk Tolerance	Moderate risk tolerance applies to structured procurements, like wireless networks at a forward deployed base. PMs should implement all previous strategies and: - Use verifiable vendor processes for product integrity (e.g., SSAE18-SOC2). - Improve awareness of vendor/product limitations. - Manage critical SCRM risks through countermeasures.
Low Risk Tolerance	Low risk tolerance applies to engineered procurements, like industrial control systems in a tank. PMs should implement all previous strategies and: - Assess critical components. - Implement available countermeasures. - Utilize commercial assessment vendors, the Joint Federated Assurance Center, interagency and close and trusted international partners, national labs/FFRDCs, and intelligence and CI.

Table 1. SCRM Actions by Risk Tolerance Level, Continued

Very Low Risk Tolerance	Very low risk tolerance applies to assured procurements, like nuclear command and control systems. PMs should implement all previous strategies and: - Follow all requirements in DoDI 5200.44 and NIST SP 800-161; including: • Conducting criticality analysis. • Documenting in Program Protection Plan. • Sending requests on critical components/suppliers to the DIA SCRM TAC or other CI sources. • Flagging reports that come back critical, high, or select medium. Utilize the scoping and mitigations process to make mitigation decisions commensurate with risk.

(4) Use assured suppliers or appropriate SCRM countermeasures for system elements that perform mission-critical functions. In accordance with DoDI 5200.44, cyber protection measures for mission-critical functions and critical components must, at minimum, include the following:

(a) Software assurance.

(b) Hardware assurance.

(c) Procurement strategies.

(d) Anti-counterfeit practices.

d. No source may be excluded from a procurement based upon SCRM considerations absent proper exercise of appropriate legal authority. Any such exclusion must be coordinated with and approved by the contracting officer and counsel.

SECTION 4: SUMMARY OF CYBERSECURITY RESOURCES

Table 2. Cybersecurity and Related Program Security Resources and Publications

Category	Title of Resource and Description
Information Protection	*FAR Clause 52.204-2* This is related to protection of information classified Confidential, Secret, or Top Secret and compliance with DoD security requirements to include the National Industrial Security Operating Manual.
Protection of Information on Networks	*FAR Clause 52.204-21* This clause is related to protection of information not intended for public release that is provided by or generated for the U.S. Government under a contract to develop or deliver a product or service to the U.S. Government, but not including information provided by the U.S. Government to the public (such as on public websites) or simple transactional information, such as necessary transactions to process payments.
	DFARS Clause 252.204-7012 The clause is related to protection and safeguarding of CDI, as defined in the clause, and reporting to the DoD of the possible exfiltration, manipulation, or other loss or compromise of unclassified CDI; or other activities that allow unauthorized access to the contractor's unclassified IS on which unclassified CDI is resident or transiting. For more information, see Guidance to Stakeholders for Implementing DFARS Clause 252.204-7012, released by the Office of the Deputy Assistant Secretary of Defense for Systems Engineering.
	DoDI 5205.13 - Establishes an approach for protecting unclassified DoD information transiting or residing on unclassified DIB ISs and networks. - Increases DoD and DIB situational awareness. - Establishes a DoD and DIB collaborative information sharing environment. - DoD CIO manages the DIB Cyber Security/ Information Assurance Program.
	Executive Order 13691 Encourages and promotes sharing of cybersecurity threat information within the private sector and between the private sector and government.
OPSEC	*DoDD 5205.02E* Establishes process for identifying critical information and analyzing friendly actions attendant to military operations and other activities to: - Identify those actions that can be observed by adversary intelligence systems. - Determine indicators and vulnerabilities that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and determine which of these represent an unacceptable risk. - Select and execute countermeasures that eliminate the risk to friendly actions and operations or reduce it to an acceptable level.
Protection of information technology and ISs	*DoDI 8500.01* Establishes a DoD cybersecurity program to protect and defend DoD information and information technology.
	DoDI 8510.01 Establishes the DoD decision process for managing cybersecurity risk to DoD information technology.
	Section 2223(a) of Title 10 U.S.C. Requires a cybersecurity strategy for programs that are considered Mission Critical and Mission Essential and includes information technology.
System Protection	*DoDI 5200.39* Provides policy and procedures for protecting CPI. CPI includes U.S. capability elements that contribute to the warfighters' technical advantage, which, if compromised, undermine U.S. military preeminence. U.S. capability elements may include, but are not limited to, software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment.
	DoDI 5200.44 Establishes policy and procedures for managing supply chain risk. A supply chain is at risk when an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

Table 3. Cybersecurity and Related Program Security Resources and Publications, Continued

Category	Title of Resource and Description
	Section 933 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013, Public Law 112-239 Requires use of appropriate automated vulnerability analysis tools in computer software code during the entire life cycle, including during development, operational testing, operations and sustainment phases, and retirement.
	Section 937 of the NDAA for Fiscal Year 2014, Public Law 113-66 Requires the DoD to establish a joint federation of capabilities to support trusted defense system needs to ensure the security of software and hardware developed, maintained, and used by the DoD.
	DoDI 8530.01 Establishes policy and assigns responsibilities to protect the DoD Information Network against unauthorized activity, vulnerabilities, or threats.
	Joint Federated Assurance Center, chartered under Section 937 of the Fiscal Year 2014 NDAA Federation of subject matter experts and capabilities to support program hardware and software assurance needs.
	National Cyber Range (NCR) The NCR is institutionally funded by USD(R&E) Test Resource Management Center to provide cybersecurity T&E as a service to DoD Customers. The NCR provides secure facilities, computing resources, repeatable processes and skilled workforce as a service to PMs. The NCR Team helps the PM plan and execute a wide range of event types including science and technology experimentation, architectural evaluations, security control assessments, cooperative vulnerability, adversarial assessments, training and mission rehearsal. The NCR creates hi- fidelity, mission representative cyberspace environments and also facilitates the integration of cyberspace T&E infrastructure through partnerships with key stakeholders across DoD, the Department of Homeland Security, industry, and academia.
Threat Assessment and Integration	*DIA* Produces intelligence and counterintelligence assessments, to include assessment of supplier threats to acquisition programs providing critical weapons, ISs, or service capabilities, and system threat intelligence reports.
	Defense Counterintelligence and Security Agency Provides the cleared U.S. defense industry with information about foreign intelligence threats; and ensures that the cleared U.S. defense industry safeguards the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts.
Threat Assessment and Integration	*Joint Acquisition Protection and Exploitation Cell* An USD(R&E) organization focusing on collaboration among the acquisition, intelligence, counterintelligence, law enforcement, and operations communities to prevent, mitigate, and respond to data loss.
Risk, Issue, and Opportunity Management	*The January 9, 2017 Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum* A guidance document that addresses the significant relationship between program success and effective risk management.
Cybersecurity T&E	*The April 3, 2018 Director of Operational Test and Evaluation Memorandum* A guidance document that describes approaches for operational cybersecurity testing.
	DoD Cybersecurity T&E Guidebook A guidance document that addresses planning, analysis, and implementation of cybersecurity T&E for chief developmental testers, lead developmental T&E organizations, operational test agencies, and the larger test community.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
AAF	adaptive acquisition framework
ATO	authority to operate
CDRUSCYBERCOM	Commander, United States Cyber Command
CIO	chief information officer
CMMC	cybersecurity maturity model certification
COTS	commercially available off-the-shelf
CUI	controlled unclassified information
DA	decision authority
DAS	Defense Acquisition System
DFARS	Defense Federal Acquisition Regulation Supplement
DIA	Defense Intelligence Agency
DIB	defense industrial base
DoDD	DoD directive
DoDI	DoD instruction
FAR	Federal Acquisition Regulation
IS	information system
MDA	milestone decision authorities
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
PIT	platform information technology
PM	program manager
RMF	risk management framework
SCRM	supply chain risk management
SP	special publication
T&E	test and evaluation
U.S.C.	United States Code
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I&S)	Under Secretary of Defense for Intelligence and Security

ACRONYM	MEANING
USD(R&E)	Under Secretary of Defense for Research and Engineering
VOLT	Validated Online Lifecycle Threat

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
cyber-contested environment	An operational environment where U.S. adversaries are known to have the capability and intent to attack the hardware, software, firmware, and communications of U.S. IS and PIT.
cyber hygiene	The use of cybersecurity controls in an operational environment to prevent successful attacks on cyber networks, computers, and application by adversaries with minimal capability and intent.
cyber incident	A cyber incident is the act of violating an explicit or implied security policy of an IS or PIT. This includes, but is not limited to: • Attempts (either failed or successful) to gain unauthorized access to a system or its data. • Unwanted disruption or denial of service. • The unauthorized use of a system for the processing or storage of data. • Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.
cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
data	A set of information in an electronic format that allows it to be retrieved or transmitted.
strategic competitors	Adversary nations, or other organizations, that bring the same amount of capability, intent, and resources to conflict, up to and including war, with the U.S. in one or more warfighting domains.
operational environment	A set of operational conditions, selected by the users, in coordination with the appropriate independent operational testing agency, that are representative of the desired spectrum of operational employments.

REFERENCES

Chairman of the Joint Chief of Staff Instruction 5123.01H, "Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS)," August 31, 2018

Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," October 2016

DoD Cybersecurity Test and Evaluation Guidebook, February 10, 2020

DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003, as amended

DoD Directive 5135.02, "Under Secretary of Defense for Acquisition and Sustainment (USD(A&S))," July 15, 2020

DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012, 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 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 & Networks (TSN)," November 5, 2012, as amended

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

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

DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology," March 12, 2014, as amended

DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," July 25, 2017, as amended

Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing," February 13, 2015

Federal Acquisition Regulation (FAR) Clause 52.204-21, "Basic Safeguarding of Covered Contractor Information Systems," June 15, 2016

National Institute of Standards and Technology Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations" January 16, 2020

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

Under Secretary of Defense for Acquisition, Technology and Logistics Memorandum, "DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs" January 9, 2017

United States Code, Title 10
United States Code, Title 44