SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

November 13, 2020

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP (SEE DISTRIBUTION)
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Directive-type Memorandum (DTM) 20-004, "Enabling Cyberspace Accountability of DoD Components and Information Systems"

References: See Attachment 1.

Purpose. This DTM:

- Provides DoD Components, at all levels, guidance for implementing effective cybersecurity (CS) practices to counter adversaries' efforts to exploit critical cybersecurity vulnerabilities that could impede or prevent DoD mission success.

- Establishes policy, assigns responsibilities, provides supplementary policy guidance, and prescribes procedures enabling cyberspace accountability within DoD to address risks assumed by commanders and directors in the cyberspace area of operations.

- Establishes CS requirements and cyberspace operational risk management functions applying to all programs, information systems, and technologies in DoD, regardless of the acquisition or procurement method (referred to collectively in this DTM as "systems").

- Establishes that all DoD personnel making decisions affecting cybersecurity, or cyber operational risk, will be held accountable, as appropriate, for those decisions.

- This DTM is effective November 13, 2020; it must be incorporated into DoD Instruction (DoDI) 8510.01. This DTM will expire effective November 13, 2021

Applicability. This DTM 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 Department of Defense (referred to collectively in this DTM as the "DoD Components").

Definitions. See Glossary.

Policy.

- Accountability for CS risk accepted within DoD must be enforced at all levels within the OSD or DoD Component in question and throughout the lifecycle of its systems in accordance with DoDIs 8500.01, 8510.01, and 3020.45, and in accordance with DoD Directive (DoDD) 3020.40.

- Risk decisions affecting CS must be mutually coordinated and include cyberspace operations forces (COF) with the affected operational authorities, as described in Attachment 3 of this DTM, whether the decisions are made by:

    - Authorizing officials (AOs) under the risk management framework (RMF) in DoDI 8510.01;

    - Acquisition program managers through program trades made within the system sustainment phase of the Defense Acquisition System lifecycle, including decisions to withhold or delay vulnerability remediation, as detailed in DoDD 5000.01 and DoDI 5000.02; or

    - Functional operational commanders.

- Cyberspace and functional operational commanders, as defined in the Glossary, and AOs are informed of system CS risks within their areas of responsibility.

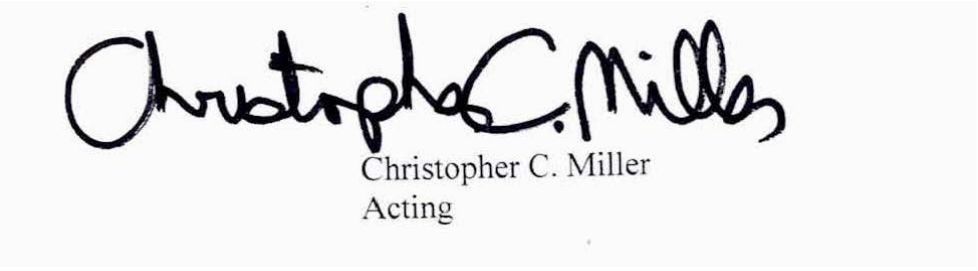
- Authoritative procedures and guidance for this DTM will be provided on the RMF Knowledge Service at https://rmfks.osd.mil.

Responsibilities. See Attachment 2.

Procedures. See Attachment 3.

Information Collection Requirements. Reporting associated with this DTM will be collected and monitored via the CS accountability scorecards, as described in Attachment 3.

Releasability. Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.



Attachments:
As stated

DISTRIBUTION:
Chief Management Officer of the Department of Defense
Secretaries of the Military Departments
Chairman of the Joint Chiefs of Staff
Under Secretaries of Defense
Chief of the National Guard Bureau
General Counsel of the Department of Defense
Director of Cost Assessment and Program Evaluation
Inspector General of the Department of Defense
Director of Operational Test and Evaluation
DoD Chief Information Officer
Assistant Secretary of Defense for Legislative Affairs
Assistant to the Secretary of Defense for Public Affairs
Director of Net Assessment

ATTACHMENT 1

REFERENCES

DoD Directive 3020.40, "Mission Assurance," November 29, 2016, as amended

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

DoD Instruction 3020.45, "Mission Assurance (MA) Construct," August 14, 2018

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

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

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

DoD Instruction 8531.01, "DoD Vulnerability Management," September 15, 2020

DoD Directive 5100.20, "National Security Agency/Central Security Service (NSA/CSS)," January 26, 2010

DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," April 21, 2016, as amended

DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, as amended

United States Code, Title 44, Section 3502

ATTACHMENT 2

RESPONSIBILITIES

1. DOD CHIEF INFORMATION OFFICER (DoD CIO). In addition to the responsibilities in Paragraph 10 of this attachment, the DoD CIO:

a. Maintains an authoritative CS accountability scorecard of the risk posture across all systems and networks both in development and in sustainment, and for review by DoD senior leaders, to help inform decision making.

b. Develops, implements, and enforces the DoD CS program.

c. In coordination with the Commander, United States Cyber Command (CDRUSCYBERCOM), integrates the DoD CS RMF program with the secure, operate, and defend functions of the DoD Information Networks mission area.

d. Coordinates with the Under Secretary of Defense for Intelligence and Security (USD(I&S)), CDRUSCYBERCOM, and other Intelligence Community (IC) stakeholders to ensure that the appropriate supporting IC organization(s) provide/make available relevant commercial and intelligence threat data to DoD Components.

e. In coordination with the Principal Cyber Advisor (PCA) and CDRUSCYBERCOM, develops and oversees CS requirements in the requirements management processes.

f. Updates policy and processes within his or her purview in accordance with this issuance.

g. In coordination with the PCA, the Chairman of the Joint Chiefs of Staff, the Director, National Security Agency (NSA), and CDRUSCYBERCOM, oversees additional areas of focus, including cyberspace metrics, to inform DoD stakeholders by leveraging the CS accountability scorecards.

2. UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT (USD(A&S)). In addition to the responsibilities in Paragraph 10 of this attachment, the USD(A&S):

a. Verifies that DoD Component acquisition program executive offices, program managers, and system owners are accountable for:

(1) Implementing CS policies and requirements throughout the system's lifecycle.

(2) Coordinating, with the requirements sponsors, AO, and component COF, regarding tradeoff decisions that significantly affect survivability of systems under conditions of the intended operational environment during sustainment of systems, including decisions to withhold or delay vulnerability remediation and mission risk mitigations.

b. Confirms that weapons systems and other defense critical infrastructure are:

(1) Sustained in accordance with the DoD CS program as outlined in this issuance and DoDI 8500.01.

(2) Appropriately integrated into the cyber operational environment under an accountable commander or command authorized official.

c. Provides the cyber risk mitigation tool as an enterprise-wide repository for tracking cyber vulnerability assessments and mitigations.

d. Updates policy and processes within their purview in accordance with this issuance.

3. UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING (USD(R&E)). In addition to the responsibilities in Paragraph 10 of this attachment, the USD(R&E):

a. Informed by operational resilience and survivability requirements in accordance with DoD policy and guidance on all Acquisition Category ID program acquisition systems, confirms that developmental testing is being performed, and that the results are integrated into the CS process as systems are being developed.

b. Confirms that research activities (initial capabilities document phase) are protected and meet CS requirements.

c. Updates policy and processes within their purview in accordance with this issuance.

4. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS. In addition to the responsibilities in Paragraph 10 of this attachment, the Under Secretary of Defense for Personnel and Readiness:

a. In conjunction with appropriate Principal Staff Assistants, requires CS as an evaluation criterion for performance for all positions with oversight, management, or supervision of CS efforts.

b. Updates policy and processes within their purview in accordance with this issuance.

5. USD(I&S). In addition to the cybersecurity-related responsibilities outlined in DoDI 8500.01, and the responsibilities in Paragraph 10 of this attachment, the USD(I&S) ensures the protection and safeguarding of cyber and cyber-related information, regardless of format, in accordance with DoDI 5200.01 and Volume 1 of DoD Manual 5200.01.

6. DIRECTOR OF THE NSA/CHIEF OF THE CENTRAL SECURITY SERVICE. Under the authority, direction, and control of the USD(I&S), in addition to the cybersecurity-related responsibilities in DoDD 5100.20, the responsibilities in DoDI 8500.01, and the responsibilities in Paragraph 10 of this attachment, the Director of the NSA/Chief of the Central Security Service:

a. In coordination with the PCA, the Chairman of the Joint Chiefs of Staff, and the DoD CIO, develops CS accountability metrics to inform DoD stakeholders using a Networks CS Accountability scorecard as described in Paragraph 4 of Attachment 3.

b. Tracks the status of all remediation efforts within enterprise CS accountability scorecards maintained in conjunction with the DoD CIO and the CDRUSCYBERCOM.

7. DIRECTOR, DEFENSE INTELLIGENCE AGENCY. Under the authority, direction, and control of the USD(I&S), and in addition to the responsibilities in Paragraph 10 of this attachment, the Director, Defense Intelligence Agency, performs CS-related responsibilities in accordance with DoDI 8500.01.

8. ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND GLOBAL SECURITY. Under the authority, direction, and control of the Under Secretary of Defense for Policy, the Assistant Secretary of Defense for Homeland Defense and Global Security, in his or her role as the PCA, and in coordination with the DoD CIO, the Chairman of the Joint Chiefs of Staff, the Director of the NSA/Chief of the Central Security Service, and the CDRUSCYBERCOM, supports additional areas of focus, including cyberspace metrics, to inform DoD stakeholders leveraging the Networks CS Accountability Scorecard capabilities.

9. DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR DEFENSE CONTINUITY AND MISSION ASSURANCE (DASD(DC&MA)). Under the authority, direction, and control of the Under Secretary of Defense For Policy, and the Assistant Secretary of Defense for Homeland Defense and Global Security, the DASD(DC&MA) coordinates all mission assurance policy to ensure that DoD can execute its core missions, consistent with DoDD 3020.40. The DASD(DC&MA):

a. Establishes and leads a comprehensive and integrated risk management governance and oversight steering group.

b. Ensures a mission assurance approach to develop and execute the DoD’s cyber strategy.

10. DOD AND OSD COMPONENT HEADS. The DoD and OSD Component heads:

a. Are responsible for establishing and providing guidance on risk tolerance within their organizations, respectively, and must comply with actions and tasks associated with CS hygiene, named cyberspace operations, and cyber operational critical task orders.

b. Implement and enforce a component CS program that:

(1) Manages system risk across a system's lifecycle.

(2) Integrates with the DoD CS program.

c. Verify that cyber intelligence and commercial cyber threat information are provided and available to systems, processes, and programs making CS or cyberspace operations related decisions.

d. Verify that system risks are documented and transparent for cyberspace and functional operational commanders and CS RM personnel throughout the system's lifecycle.

e. Prioritize CS and cyber operational requirements and functional mission requirements within systems commensurate with each requirement's impact on operations.

f. Confirm that resourcing for CS and mission assurance requirements, including mitigations, are:

(1) Incorporated into component acquisition programs and contracts.

(2) Appropriately prioritized for all systems throughout their lifecycles.

(3) Prioritized systems or assets identified as or supporting Defense Critical Infrastructure.

g. Verify that CS requirements are incorporated into systems design and CS risks are proactively identified in systems development and sustainment in accordance with DoDI 8531.01 and DoDI 8500.01.

h. Verify that CS risk acceptance decisions are made in a mutually coordinated manner and in coordination with component COF as described in Attachment 3, whether they are made by:

(1) Component AOs under the RMF described in DoDI 8510.01;

(2) Component acquisition officials through engineer tradeoffs made with sustainment of phases of the Defense Acquisition System lifecycle, including decisions to withhold or delay vulnerability remediation, in accordance with DoDD 5000.01 and DoDI 5000.02; or

(3) Functional operational commanders.

i. Hold component personnel accountable for CS and cyber operational outcomes and perform CS and cyberspace operations evaluation criteria for their performance.

j. Verify component compliance with the CS accountability scorecard and metrics reporting requirements.

k. Update component policy and processes within their purview in accordance with this issuance.

l. Through their component acquisition and sustainment authorities, confirm:

(1) That CS and cyber operational risk mitigation and vulnerability remediation, in accordance with DoDI 8531.01, are implemented and prioritized in systems throughout the system's operation and sustainment.

(2) That CS and cyber operational risk decisions are coordinated with component CS, cyberspace, and functional operational officials. The decisions are tracked, and decision-makers are accountable for cyber outcomes.

(3) That AOs are aware of the system CS vulnerabilities discovered and that mitigation plans and timelines are coordinated with cyberspace and functional operational commanders in accordance with DoDI 8531.01.

11. CHAIRMAN OF THE JOINT CHIEFS OF STAFF. In addition to the responsibilities in Paragraph 10 of this attachment, the Chairman of the Joint Chiefs of Staff:

a. Facilitates implementation of CS requirements in the Joint Capabilities Integration and Development System (JCIDS) process.

b. Enforces adequate priority of cyberspace requirements, including cyber survivability, in tradeoff decisions with other functional operational requirements within JCIDS.

c. In coordination with the DoD CIO, the PCA, the Director, NSA, and CDRUSCYBERCOM, supports additional areas of focus, including cyberspace metrics, to inform DoD stakeholders leveraging the CS accountability scorecard capabilities.

12. CDRUSCYBERCOM. In addition to the responsibilities in Paragraph 10 of this attachment, the CDRUSCYBERCOM:

a. Coordinates and oversees the cyberspace operational command framework based on authorities derived from the Unified Command Plan.

b. Oversees and confirms that designated and accountable operational commanders and directors are actively managing CS and mission risks within their assigned areas of operations.

c. Oversees and confirms that operational assessment and inspection results and trends are integrated into cyberspace risk assessment and management processes.

d. In coordination with the DoD CIO, develops, oversees, and enforces cyberspace requirements in the requirements management processes.

e. In coordination with the PCA, the Chairman of the Joint Chiefs of Staff, the DoD CIO, and the Director of the NSA/Chief of the Central Security Service, develops network CS accountability metrics to inform DoD stakeholders with a Networks CS Accountability Scorecard as described in Paragraph 4 of Attachment 3.

f. Provides all cyberspace and functional operational commanders (i.e., other Combatant Commands) awareness of any significant cybersecurity risks.

ATTACHMENT 3

PROCEDURES

1. INTEGRATION OF PROCESSES, DECISION MAKING, AND ENSURING ACCOUNTABILITY.

a. DoD has established processes, decision points, and governance structures that oversee systems development and sustainment, CS risk management and cyberspace operations, mission assurance, and other functional operational processes. These efforts are to eliminate isolated processes and decisions and to reduce significant operational risks to DoD.

b. Decision-makers in these processes (e.g., executive program officers, program managers (PMs), AOs, and cyberspace and functional operational commanders) must integrate and coordinate their decision making as described in this attachment. Additionally, these decision-makers must be held accountable for their decisions and their impact on cyberspace operations and CS.

c. To realize this outcome, DoD will better integrate system development, acquisition and sustainment processes, cyberspace operations, functional operational processes, and assessments through more effective coordination and transparency. Where necessary, escalation procedures will be presented to resolve disputes among these processes to ensure DoD mission assurance.

2. SYSTEMS OPERATIONS AND SUSTAINMENT PHASE.

a. Decision Makers. The decision-makers for the operations and sustainment phase are executive program officers, PMs, requirements sponsors, systems owners, cyberspace and functional operational commanders, AOs, or equivalent authorities.

b. Decisions. Decision-makers will determine system authorization, system vulnerability management, and alignment with CS service providers and COF.

c. Actions. DoD Component acquisition, sustainment, and CS personnel will:

(1) Continue to meet CS and cyberspace operations requirements and adequately resource these requirements throughout the system sustainment and operational phases. AOs and cyber operational commanders must ensure tailored, specific guidance for the systems and update that guidance as needed.

(2) Through their AO, authorize the system to operate. The AO will:

(a) Coordinate authorization activities and results with the system acquisition or procurement representatives.

(b) Ensure the system meets cyberspace operational commander requirements. When risks are not fully mitigated, inform operators of potential impacts.

(c) Ensure the cyberspace and functional operational commanders have the necessary cyber risk information on the system.

(d) When a cyber-system risk affects an operational requirement, facilitate coordination with:

1. Cyberspace and functional operational commanders.

2. Acquisition or procurement representatives.

(e) Ensure that decisions:

1. Incorporate the best cyber intelligence or commercial cyber threat information available.

2. Are recorded, tracked, and made available to all parties throughout the system's lifecycle.

(3) Identify system vulnerabilities affecting CS or cyberspace operations and initiate, prosecute, track, and complete the vulnerability remediation process in accordance with DoDIs 8510.01, 8531.01, and 3020.45. Remediation and mitigation plans and decisions must be coordinated among PMs, requirements sponsors, AOs, and cyber and functional operational commanders. However, AOs make the final cyber risk decision affecting the CS posture of the system.

(4) Implement process and governance mechanisms to resolve disputes, elevate concerns as necessary, and ensure accountability for outcomes.

(5) Track the status of all remediation efforts within enterprise CS accountability scorecards maintained by the DoD CIO, the USD(A&S), the Director, NSA, and the CDRUSCYBERCOM.

3. MANDATED PROCESS UPDATES.

a. The DoD CIO will update DoDI 8500.01 to incorporate all CS activities and requirements into the DoD CS Program and establish how CS will be integrated with other processes. To ensure integration between the DoD CS Program and relevant DoD systems, the following components will coordinate with the DoD CIO:

(1) United States Cyber Command, to ensure integration with the United States Cyber Command operational command framework.

(2) Office of the USD(A&S), to ensure integration with the DoD Acquisition and Sustainment Lifecycle Process.

(3) Office of the USD(R&E), to ensure integration with DoD research, development, and engineering processes.

(4) Office of the Chairman of the Joint Chiefs of Staff, to ensure integration with the JCIDS process.

(5) Office of the USD(P), to ensure integration with mission assurance processes.

b. The DoD CIO will update the CS authorization process contained in DoDI 8510.01 to ensure that the best intelligence and threat information are being used throughout the security authorization process.

(1) The security authorization process will be updated to ensure that:

(a) Cyberspace operational commanders and directors are informed of systems and risks in their areas of operations.

(b) The security authorization process meets cyberspace operational commanders' requirements.

(2) United States Cyber Command direction is incorporated into security authorization baselines as required.

4. CS ACCOUNTABILITY SCORECARDS.

a. DoD will assess all DoD Components with a Networks CS Accountability Scorecard. The initial Networks CS Accountability Scorecard includes, but is not limited to, the following metric categories:

(1) Named Operations. This metric will assess a DoD Component's compliance with completing select critical tasks associated with a deliberately planned CDRUSCYBERCOM operation. Key named operation task metrics will change over time. The critical tasks are based on proactive efforts aimed at preserving mission assurance and preventing serious damage to national security. The time compliance window for completing critical tasks associated with a planned operation will vary from immediate action to executing within a specified time.

(2) Critical Cyber Taskings. This metric will assess a DoD Component's compliance with completing critical cyber tasks. Critical cyber tasks are based on known vulnerabilities, threat-informed intelligence, and other sources. They will change over time as new vulnerabilities are discovered. Tasks not completed as directed result in unmitigated vulnerabilities, which could jeopardize mission success or cause serious damage to national security. Critical cyber taskings must be completed immediately.

(3) Security Posture. This metric will assess a DoD Component's compliance with selected CS hygiene metrics derived from the DoD CS hygiene and DoD Top 10 scorecards. The time window for correcting CS hygiene metrics found to be non-compliant varies from "immediately" to "within a specified time."

(4) Assessments and Inspections. This metric will be a rolling average of the three most recent years of a component's score for command cyber operations readiness and cyber readiness inspections.

b. Scorecard metrics will change over time in response to the threats and vulnerabilities. These scorecards enable leaders to make informed decisions regarding the allocation of cyber resources and to hold DoD Component personnel accountable for the CS of systems.

ATTACHMENT 4

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ACRONYM	MEANING
AO	authorizing official
CDRUSCYBERCOM	Commander, United States Cyber Command
COF	cyberspace operations forces
CS	cybersecurity
DASD(DC&MA)	Deputy Assistant Secretary of Defense for Defense Continuity and Mission Assurance
DoD CIO	DoD Chief Information Officer
DoDD	DoD directive
DoDI	DoD instruction
DTM	directive-type memorandum
JCIDS	Joint Capabilities Integration and Development System
NSA	National Security Agency
PCA	Principal Cyber Advisor
PM	program manager
RMF	risk management framework
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(R&E)	Under Secretary of Defense for Research and Engineering

PART II. DEFINITIONS

TERM	DEFINITION
cyberspace operational commander	Operational commander with responsibility for cyberspace operations within a specific area of operations.
functional operational commander	Operational commander with responsibility for operations for a business or mission area outside cyberspace.
information system	As defined in Section 3502 of Title 44, U.S. Code.