



DEPARTMENT OF DEFENSE

6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

February 27, 2024

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Directive-type Memorandum (DTM) 24-001 – “DoD Cybersecurity Activities Performed for Cloud Service Offerings”

References: See Attachment 1.

Purpose. In accordance with the authority in DoD Directive (DoDD) 5144.02, this DTM:

- Establishes policy, assigns responsibilities, and provides procedures for cybersecurity and defensive cyberspace operations (DCO) activities that are performed on DoD systems and technology by a cybersecurity service provider (CSSP), DoD entity, or commercial entity on behalf of the mission owner or authorizing official.
- Incorporates and cancels DoD Chief Information Officer (DoD CIO) Memorandum, “Department of Defense Cyber Security Activities Performed for Cloud Service Offerings,” November 15, 2017.
- Is effective February 27, 2024; it must be incorporated into DoD Instruction (DoDI) 8530.01 and DoD Manual 8530.01. This DTM will expire effective February 27, 2025

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 DoD (referred to collectively in this DTM as the “DoD Components”).

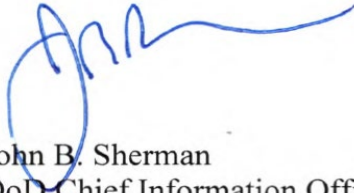
Definitions. See Glossary.

Policy. The DoD will identify, protect, detect, respond, and recover DoD information, systems, and technology.

Responsibilities. See Attachment 2.

Procedures. See Attachment 3.

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



John B. Sherman
DoD Chief Information Officer

Attachments:
As stated

ATTACHMENT 1

REFERENCES

- Chairman of the Joint Chiefs of Staff Manual 6510.01, “Cyber Incident Handling Program,” current edition
- Committee on National Security Systems Policy 32, “Policy on Cloud Computing,” May 2022
- Chairman of the Joint Chiefs of Staff Execute Order, “Modification to Execute Order To Implement Cyberspace Operations Command and Control,” November 14, 2014
- Code of Federal Regulations, Title 36, Subpart 1222.32
- Committee on National Security Systems Instruction No. 4009, “Committee on National Security Systems (CNSS) Glossary,” March 2, 2022
- Defense Federal Acquisition Regulation Supplement, Subpart 204.73, current edition
- Defense Information Systems Agency, “DoD Cloud Computing Security Requirements Guide,” current version¹
- DoD Deputy Chief Information Officer, “DoD Architecture Framework Version 2.02,” August 2010²
- DoD Directive 5106.01, “Inspector General of the Department of Defense (IG DOD),” April 20, 2012, as amended
- DoD Directive 5144.02, “DoD Chief Information Officer (DoD CIO),” November 21, 2014, as amended
- DoD Directive 5205.16, “The DoD Insider Threat Program,” September 30, 2014, as amended
- DoD Directive 8000.01, “Management of The Department of Defense Information Enterprise (DoD IE),” March 17, 2016, as amended
- DoD Instruction 5200.48, “Controlled Unclassified Information (CUI),” March 6, 2020
- DoD Instruction 8330.01, “Interoperability of Information Technology, Including National Security Systems,” September 27, 2022
- DoD Instruction 8500.01, “Cybersecurity,” March 14, 2014, as amended
- DoD Instruction 8530.01, “Cybersecurity Activities Support to DoD Information Network Operations,” March 7, 2016, as amended
- DoD Instruction 8530.03, “Cyber Incident Response,” August 9, 2023
- DoD Instruction 8531.01, “DoD Vulnerability Management,” September 15, 2020
- DoD Instruction 8582.01, “Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information,” December 9, 2019
- DoD Manual 8530.01, “Cybersecurity Activities Support Procedures,” May 31, 2023
- Executive Order 14028, “Improving the Nation’s Cybersecurity,” May 12, 2021
- National Institute of Standards and Technology Special Publication, “NIST Cloud Computing Reference Architecture,” September 2011

¹ Available at https://dl.dod.cyber.mil/wp-content/uploads/cloud/zip/U_Cloud_Computing_SRG_V1R4.zip

² Available at <https://dodcio.defense.gov/Library/DoD-Architecture-Framework/>

- National Institute of Standards and Technology Special Publication 500-292, “NIST Cloud Computing Reference Architecture,” September 2011
- National Institute of Standards and Technology Special Publication 800-137, “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,” September 30, 2011
- National Security Directive 42, “National Policy for the Security of National Security Telecommunications and Information Systems,” July 5, 1990
- National Security Memorandum-08, “Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems,” January 19, 2022
- Office of Management and Budget Circular A-130, “Managing Information as a Strategic Resource,” July 28, 2016
- United States Cyber Command Instruction 5200-13, “Cyberspace Protection Conditions (CPCON),” April 13, 2019

ATTACHMENT 2
RESPONSIBILITIES

1. DOD CIO. The DoD CIO:

- a. Provides strategic management, guidance, and direction to DoD Component efforts to plan, program, budget, develop, and implement the capability to protect the Department of Defense Information Network (DODIN) based on the DoD Enterprise Architecture in accordance with DoDD 8000.01 and the evolving Joint Information Environment architecture.
- b. Ensures capabilities are developed and incorporated into the DoD Information Enterprise Architecture in accordance with DoDI 8330.01 to protect the DODIN.
- c. Oversees the development and implementation of DoD cybersecurity architectures and capabilities to protect the DODIN, in coordination with Commander, United States Cyber Command (CDRUSCYBERCOM), Director of National Security Agency, and Chief Central Security Service as National Manager.
- d. Implements directed actions in accordance with cyber tasking orders (TASKORDs) or other directives issued through the United States Cyber Command (USCYBERCOM) or subordinate Commander, Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN) in accordance with the November 14, 2014 Chairman of the Joint Chiefs of Staff Execute Order.

2. DOD COMPONENT HEADS. In addition to the responsibilities in DoDI 8530.01, the DoD Component heads ensure the mission owner is responsible and authorizing official is accountable, for:

- a. Ensuring all cloud service offering (CSO) contracts include accreditation boundaries and licensing agreements for cybersecurity activities.
- b. Ensuring all CSO contracts include requirements for CSSP notification and acknowledgement procedures for cyber incidents.
- c. Ensuring independent, threat-representative cyber testing is integrated into all CSO contracts and performed by a certified and accredited DoD Cyber Red Team (DCRT), in accordance with DoDI 8330.01. More advanced capability testing and integration within contested and congested cyberspace conditions is encouraged.
- d. Establishing processes and validating agreements and tactics, techniques, and procedures (TTPs) between mission owners, CSSPs, and CSOs for CSO-related incident response.
- e. Ensuring that Component cybersecurity policies:

(1) Specify that the cognizant mission owner retains responsibility for commercial entity performance.

(2) Identify processes for approving and tracking corrective actions for CSOs, and that those processes are also included in CSO contracts.

ATTACHMENT 3

DOD CLOUD CYBERSECURITY ACTIVITIES

1. MISSION OWNER. The mission owner:

a. Ensures the data that is migrated to the cloud is at the appropriate security level. Having approval from their risk management executive or authorizing official is required for establishing a formal agreement or contract to document acquired cybersecurity services for mission owner data and systems hosted within a CSO. The formal agreement or contract must detail the arrangement and expectations between the mission owner, CSSP, DoD entity, or commercial entity for establishing, measuring, and maintaining a required level of performance and delivery of the respective compliance artifacts. Formal agreements and contracts may require explicit service level agreements when specific regulatory directives do not exist.

b. Before accepting a cybersecurity activity that a commercial entity performs, and in coordination with their DoD Component authorizing official, ensures JFHQ-DODIN can evaluate and assess the cybersecurity activities. Mission owners and their authorizing official must review the Federal Risk and Authorization Management Program (FedRAMP) and DoD provisional authorization artifacts associated with the mission owner cloud environment to understand the risks that the mission will inherit when using the selected CSO for the mission system or application.

(1) The mission owner needs the authorizing official to accept and manage the risk of supported cybersecurity activities and identify any gaps in cybersecurity activities.

(2) An authorizing official must consider the risk and validate who will be responsible for providing each cybersecurity activity and address gaps at an acceptable level of risk associated to the level of protection required for any hardware, software, or data hosted in a cloud environment.

(3) The mission owner, program manager (PM), and authorizing official must review, accept, and document selected cloud service provider (CSP) cybersecurity services and supporting evaluations as part of a DoD provisional authorization or other DoD authorization. These artifacts form the basis of reciprocity.

c. Ensures contractual language specifies and documents a CSP's compliance requirement to provide data identified to meet CSSP DCO requirements and share this information to all parties involved in defending DoD data in the cloud, including the designated CSSP, authorizing official, and DoD sponsor, when required.

d. Provides access to capabilities, assets, and data of supporting DoD entities and commercial entities to the DoD inspection and assessment team(s). The DoD entity and commercial entity will grant access and permissions to the mission owner, PM, authorizing official, CSSP, and DoD inspection and assessment team(s). Access to all cybersecurity related information that DoD entities and commercial entities collect would be restricted to only those required to perform the cybersecurity activities on behalf of the DoD.

2. CYBERSECURITY ACTIVITIES.

a. The mission owner will address and ensure the performance of all activities listed in Table 1. The table reflects three annotations to specify the organizations that may perform the cybersecurity activity for each service model (i.e., infrastructure as a service (IaaS), platform as a service (PaaS), or software as a service (SaaS)) by impact level (IL) (i.e., 2, 4/5, or 6). Cybersecurity activities conducted on a system identified as a national security system or connected to a national security system, are required to be in accordance with Committee on National Security Systems Policy 32, National Security Directive 42, Executive Order 14028 and National Security Memorandum-08.

b. If the cybersecurity activity is not specifically listed, refer to DoDI 8530.01.

Table 1. Cybersecurity Activities Table

Cybersecurity Activities		IaaS			PaaS			SaaS		
		IL 2	IL 4/5	IL 6	IL 2	IL 4/5	IL 6	IL 2	IL 4/5	IL 6
Identify	Vulnerability Assessment and Analysis (VAA)									
	External Vulnerability Scans (EVS)	O	O	O	O	O	O	O	O	O
	Web Vulnerability Scans (WVS)	O	O	O	O	O	O	O	O	O
	External Assessment (Annual Assessment – See Paragraph 3.a.(2))									
	DCRT Operations	●	●	●	●	●	●	●	●	●
	DCAT Operations	O	O	O	O	O	O	O	O	O
	Penetration Testing	O	O	O	O	O	O	O	O	O
	Intrusion Assessment	O	O	O	O	O	O	O	O	O
Protect	Awareness and Training	O	O	O	O	O	O	O	O	O
	Endpoint Security Capabilities	O	O	O	O	O	O	O	O	O
	Vulnerability Management Maintenance									
	Apply DoD required security configurations	O	O	O	O	O	O	O	O	O
	Perform actions to mitigate potential vulnerabilities or threats	O	O	O	O	O	O	O	O	O
	Monitor Vulnerability Management Compliance	O	O	O	O	O	O	O	O	O
	Malware Protection	O	O	O	O	O	O	O	O	O

Table 1. Cybersecurity Activities Table, Continued

Cybersecurity Activities		IaaS			PaaS			SaaS		
		IL 2	IL 4/5	IL 6	IL 2	IL 4/5	IL 6	IL 2	IL 4/5	IL 6
Monitor and Detect	Attack Sensing and Warning (AS&W) for Anomalous Events									
	AS&W for Boundary Cyberspace Protection (BCP) Functions	N/A	●	●	N/A	●	●	N/A	●	●
	AS&W at the Application	○	○	○	○	○	○	○	○	○
	Warning Intelligence	●	●	●	●	●	●	●	●	●
	Information Security Continuous Monitoring (ISCM)									
	Maintain continuous visibility into endpoint devices	○	○	○	○	○	○	○	○	○
	Correlate asset and vulnerability data with threat data	★	★	★	★	★	★	★	★	★
	Malware Notification	★	★	★	★	★	★	★	★	★
	Detection Processes									
	Network Security Monitoring and Intrusion Detection for BCP Functions	N/A	★	★	N/A	★	★	N/A	★	★
	Network and Endpoint Security Monitoring at the Enclave Level	○	○	○	○	○	○	○	○	○
	DODIN User Activity Monitoring (UAM) for DoD Insider Threat Program									
	Employ UAM capabilities to detect anomalous insider activity	○	○	●	○	○	●	○	○	●
	Maintain insider threat audit data	○	○	○	○	○	○	○	○	○
	Correlate insider threat audit data with Component Insider Threat Programs	●	●	●	●	●	●	●	●	●
	Cyber Protection Condition (CPCON) and Orders (e.g. TASKORD, Operational Order (OPORD), Fragmentation Order)									
	CPCON and Orders Implementation	○	○	○	○	○	○	○	○	○
	CPCON and Orders Notification and Assistance	★	★	★	★	★	★	★	★	★
Respond	Incident Categorization	★	★	★	★	★	★	★	★	
	Incident Reporting	★	★	★	★	★	★	★	★	
	Incident Handling Response	○	○	○	○	○	○	○	○	
	Incident Response – Law Enforcement (LE)	★	★	★	★	★	★	★	★	
	Incident Response – Counterintelligence	★	★	★	★	★	★	★	★	
	Incident Response – Analysis	★	★	★	★	★	★	★	★	
KEY										
"★" = CSSP must perform this cybersecurity activity										
"●" = DoD entity must perform this cybersecurity activity; commercial entity cannot be performing this activity										
"○" = DoD entity or commercial entity can perform this cybersecurity activity										
"N/A" = Not Applicable										

c. A cybersecurity activity tracking checklist, generated by the mission owner and PM, will be developed in coordination with the CSSP, PM, and the authorizing official to identify who will be responsible for providing the cybersecurity activity that best fits the needs of the mission owner. The mission owner will ensure the provider performs their activities in accordance with the DoD Cloud Computing Security Requirements Guide (see DoD Manual 8530.01 for complete definitions of cybersecurity activities).

3. CYBERSECURITY ACTIVITY DESCRIPTIONS.

a. Identify. The mission owner is responsible for maintaining an inventory of mission components and providing it to the authorizing official and CSSP for required security activities listed in Table 1.

(1) Vulnerability Assessment and Analysis (VAA). The organization performing VAA must comply with the mission owner's process to request and allow the execution of any of the VAA activities.

(a) External Vulnerability Scan (EVS). A DoD entity or commercial entity can perform an EVS. The intent is to identify externally accessible vulnerabilities that may expose mission owner's data through external scans. A DoD or commercial entity performing an EVS will:

1. Send scan notifications to the mission owner and the CSSP.
2. Analyze and provide an executive summary for each scan to the mission owner and the CSSP to determine potential impacts to the mission owner's operations and will identify and mitigate or remediate the identified findings.
3. Maintain results locally and share the results of all such assessments and provide situational awareness to the mission owner, authorizing official, and the CSSP of any known vulnerabilities, mitigation strategies, and major changes to the mission owner environment upon request.

(b) Web Vulnerability Scan (WVS). A DoD entity or commercial entity can perform a WVS. The WVS is used to assist the mission owner in complying with DoDI 8530.01 for public facing web presence and with protecting DoD demilitarized zone whitelisted websites. A DoD or commercial entity performing a WVS will:

1. Provide results to the mission owner and the CSSP.
2. Analyze impacts to the DODIN for each scan and provide an executive summary to the mission owner and the CSSP. The entity will identify and mitigate or remediate the identified findings.
3. Use DoD Component approved procedures to test and evaluate WVS tools on their effectiveness, appropriateness, and safety before use on mission owner systems.

4. Provide situational awareness reports to the mission owner and CSSP of any known vulnerabilities, mitigation strategies, and major changes to the environment.

(2) External Assessment. In coordination with the PM and authorizing official, the mission owner will identify the need for external assessments, the most appropriate type of external assessment, and possible sources for the external assessments. The DoD or a commercial entity can perform the external assessment. Contracts with CSPs must include a description of the accreditation boundary and licensing agreements for DoD Cyber Assessment Team (DCAT) events and penetration tests. The organization performing external assessments must support mission owners with coordinating these activities.

(a) General. The DoD or commercial entity required to perform external assessments, as stated below, will:

1. Coordinate remote assessments with their mission owner before their command cyber readiness and command cyber operational readiness inspections.

2. Comply with the process and execution of any of the external assessment activities.

3. Supply technical assistance and report artifacts and situational awareness for external assessments within the mission owner environment to the mission owner, DoD Component authorizing official, and the CSSP.

4. Analyze and remediate identified vulnerabilities in an after-action report that details the exploited vulnerable points of the in-scope targets, with general remediation recommendations.

5. Maintain results locally and share the results with the mission owner, DoD Component authorizing official, and the CSSP.

(b) DCRT Operations.

1. A DoD certified and accredited DCRT must perform such operations. A commercial entity or other DoD entity cannot perform this activity.

2. DCRT operations identify exposed information and vulnerabilities of the DoD's security posture.

3. The DCRT report will include all findings from the exercise or network assessment based on specific mission requirements and discovered vulnerabilities, highlight any significant vulnerabilities discovered during the operation, and provide an analysis of the potential and exploited vulnerabilities discovered.

4. The requesting DoD Component then must release the report(s) to JFHQ-DODIN within 30 calendar days of the briefing.

5. The mission owner must include a description of its implementation accreditation boundary for DCRT operations contracts with CSPs.

(c) Non-DCRT Operations. A DoD entity or commercial entity can perform DCAT events and penetration tests operations. The use of cyber penetration testing teams provides real-world attack simulations designed to assess and significantly improve the effectiveness of an entire information security program.

1. The DoD or commercial entity performing non-DCRT operations will:

a. Prepare a detailed description, including architectural diagrams, of the DCAT events and penetration tests operation to the mission owner and the CSSP.

b. Obtain written approval from the mission owner to perform or conduct DCAT events and penetration tests operation.

c. Ensure basis of constraints are on safety, real-world mission execution, and operational security.

d. Coordinate all planning efforts with the requesting mission owner.

e. Deliver a detailed description of the DCAT events and penetration tests operation to the mission owner and the CSSP for approval.

f. Before mission execution, provide mission details to JFHQ-DODIN. DoD entities must submit all mission details to JFHQ-DODIN in accordance with JFHQ-DODIN reporting procedures. Commercial entities must provide this information to the mission owner to submit to JFHQ-DODIN.

g. Provide results that detail the exploited vulnerable points of the in-scope targets with general remediation recommendations to the mission owner, JFHQ-DODIN, and the CSSP for action.

2. The PM or information security system manager will execute approved corrective actions and mitigations and report actions to the mission owner, authorizing official, and CSSP for identified vulnerabilities. Contracts with CSPs must include a description of the accreditation boundary and licensing agreements for DCAT events and penetration tests operations.

(d) Penetration Testing. A DoD or commercial entity can perform penetration testing. Under mission owner direction, the assessors will attempt to breach the security features of an application, system, or network in a controlled manner. A commercial entity must demonstrate that it can perform penetration testing within DoD standards and requirements during its FedRAMP authorization. The DoD or commercial entity performing penetration testing will:

1. Deliver a detailed description of the penetration test to the mission owner and the CSSP.

2. Review mission objectives submitted by the entity (e.g., systems and networks), safety guidelines, and restraints or constraints on penetration test operations. Ensure basis of constraints are on safety, real-world mission execution, and operational security.

3. Coordinate all planning efforts with the requesting mission owner. Obtain written approval from the mission owner to perform or conduct penetration test.

4. Send the results that detail the exploited vulnerable points of the in-scope targets with general remediation recommendations to the mission owner and the CSSP.

5. Provide mission details to JFHQ-DODIN and create and disseminate lessons learned to the mission owner and the CSSP.

a. DoD entities must submit all mission details directly to JFHQ-DODIN in accordance with JFHQ-DODIN reporting procedures.

b. Commercial entities must provide this information to the mission owner to submit to JFHQ-DODIN.

6. Track and execute approved corrective actions and mitigations for identified vulnerabilities and report actions to the mission owner and CSSP.

(e) Intrusion Assessment. A DoD entity or commercial entity can perform an intrusion assessment. The assessment team is responsible for discovering malicious activity and quarantining the threat of the mission owner's network. The DoD or commercial entity performing the intrusion assessment will:

1. Perform activities identified by the CSSP at the direction of the mission owner.

2. Demonstrate that the entity can effectively, and within DoD standards and requirements, perform intrusion assessments as part of their incident handling capabilities during their FedRAMP authorization.

3. Send a detailed description of support to the authorizing official to facilitate this assessment procedure.

4. Send the results and remediation recommendations to the mission owner and CSSP.

b. Protect. These activities are performed to ensure mission enabled delivery of critical mission-services.

(1) Awareness and Training. A DoD entity or commercial entity can perform awareness and training. DoD can choose to perform the training itself or outsource the training to a commercial entity. DoD's responsibility for outsourced training is to develop the training requirement, provide compliance oversight, and develop the criteria for measuring effectiveness.

(2) Endpoint Security Capabilities. A DoD entity or commercial entity can perform endpoint security capabilities. The DoD or commercial entity providing endpoint security capabilities will:

(a) Implement and maintain endpoint security software.

(b) Ensure audit and log records are determined, documented, implemented, and reviewed in accordance with DoD policies and issuances, the mission owner policies, and the Cybersecurity Reference Architecture in DoD Cloud Computing Security Requirements Guide.

(c) Report the detection of alerts from the endpoint security software to the authorizing official or CSSP.

(d) Distribute endpoint configurations and enforce compliance policies as directed by the mission owner and with the authorizing official's approval.

(e) Ensure audit and log records and any endpoint intrusion detection system logs are available as required for the CSSP.

(3) Vulnerability Management Maintenance. Supporting the vulnerability management program in accordance with DoDI 8531.01, is not a DoD-specific activity. Any contract with a commercial entity must require submission of all reports and supporting documentation to the mission owner and the CSSP.

(a) Apply DoD Required Security Configurations. A DoD entity or commercial entity can apply DoD-required security configurations. The DoD or commercial entity applying DoD required security configurations will establish a comprehensive vulnerability management plan the authorizing official approves.

(b) Perform Actions to Mitigate Potential Vulnerabilities or Threats. A DoD entity or commercial entity can perform actions to mitigate potential vulnerability or threats. The DoD or commercial entity performing such actions will provide an analysis of the correlation between the vulnerability management status of assets and malicious incidents to the mission owner and the identified CSSP.

(c) Monitor Vulnerability Management Compliance. A DoD entity or commercial entity can monitor vulnerability management compliance. The DoD or commercial entity monitoring such compliance will produce required documentation, ensure timely reporting of compliance statistics for each cybersecurity vulnerability management directives and USCYBERCOM TASKORDs to the mission owner, and aggregate acknowledgement and compliance reports.

(4) Malware Protection. A DoD entity or commercial entity can perform malware protection.

(a) The mission owner is responsible and the authorizing official is accountable for ensuring that the organization performing malware protection will:

1. Have documented procedures on reporting of malware to the mission owner.

2. Provide detailed reports immediately following all malware incidents.

3. Annually provide a trending analysis report from malware incidents to the mission owner and the authorizing official.

(b) The DoD or commercial entity performing malware protection will:

1. Establish the capability to capture, correlate, analyze, and provide continuous visibility into DoD assets.

2. Assess the compliance, effectiveness, and changed state of security controls protecting the DoD Component-owned or -operated system(s) and application(s) and data.

3. Maintain ongoing awareness of information security, threats, and vulnerabilities to support organizational risk management decisions.

4. Support DODIN operations by providing ongoing awareness of threats and security status of traffic, fault, performance, bandwidth, route, and associated network management areas.

5. Support monitoring for anomalous activity.

6. Implement the capability to detect and prevent malware incidents by employing malware detection and remediation mechanisms to detect and remove malicious code.

7. Contain the spread of malware to prevent further damage and eradicate the malware from infected hosts.

8. Employ mitigating actions to prevent reinfection and restore functionality.

9. Configure malware detection mechanisms to perform periodic scans of the mission owner's environment in accordance with current DoD and DoD Component guidance.

10. Maintain and access anti-virus and anti-malware software for latest updates and releases.

11. Support virus responses and self-reporting 24/7.

12. Ensure proper protection of data at rest and data in transit, in accordance with applicable DoD policies.

13. Track and execute corrective actions as appropriate and report actions to the mission owner and the CSSP point of contact (POC).

c. Monitor and Detect. This activity is conducted to support the DoD Component's execution of missions, through attack sensing and warning (AS&W) mission-enabled capabilities as defined in Committee on National Security Systems Instruction No. 4009.

(1) AS&W for Anomalies and Events.

(a) AS&W for Boundary Cyberspace Protection (BCP). A DoD entity must perform AS&W for BCP. A commercial entity cannot perform it. USCYBERCOM must authorize the DoD entity performing AS&W for BCP functions.

1. The DoD entity will perform AS&W functions at the Defense Information Systems Network ingress and egress points connecting to commercial CSP environments.

2. This activity is not applicable for IL2 CSO due to the traffic in IL2 not required to pass through the Internet Access Point or Boundary Cloud Access Points per the DoD Cloud Computing Security Requirements Guide.

(b) AS&W at the Application. A DoD entity or commercial entity can perform AS&W at the application. The DoD or commercial entity performing AS&W at the application will:

1. Capture and identify events leading to incident identification and alerting through automated means.

2. Immediately report all security violations of unauthorized user activity to the mission owner.

3. Gather and assess logs and artifacts as well as other criteria, including direction of traffic flow, configurations, previous investigation results, ports, protocols, and services, and traffic vetted as authorized by a subscriber.

4. Track and execute actions as appropriate and report actions to the mission owner and CSSP POC.

(c) Warning Intelligence. This activity is used to distribute relevant warning intelligence relating to DoD information systems and computer networks received from

intelligence sources to DoD entities for situational awareness. This activity must be performed by a DoD entity and cannot be performed by a commercial entity. DoD entities must provide sufficient information to the organization performing warning intelligence to affect changes and enhance DCO and resiliency.

(2) Information Security Continuous Monitoring (ISCM). When detecting an incident or event, the U.S. Government must declare the category and severity, as well as file and safeguard the reports for future analysis by the CSSP. More guidance on ISCM is in DoDI 8500.01, DoD Manual 8530.01, and National Institute of Standards and Technology Special Publication 800-137. The mission owner will ensure visibility into endpoint devices for any organization to perform ISCM.

(a) Maintain Continuous Visibility into Endpoint Devices. A DoD entity or commercial entity can perform this activity. The DoD or commercial entity maintaining continuous visibility into endpoint devices will:

1. Establish the capability to capture, correlate, analyze, and provide continuous visibility into DoD assets.

2. Assess the compliance, effectiveness, and changed state of security controls protecting the DoD Component-owned or -operated system(s), application(s) and data.

3. Report changes in the state of security controls to the mission owner and the identified CSSP POC.

4. Support DODIN operations by providing continuous awareness of threats and security status of traffic, fault, performance, bandwidth, route, and associated network management areas via the CSSP.

5. Monitor employee activity to detect anomalous occurrences.

6. Maintain continuous awareness and security status of reportable cyber events and incidents to support timely, informed, and actionable cyber incident handling decisions and report all threats to the mission owner and the CSSP POC.

(b) Correlate Asset and Vulnerability Data with Threat Data. A CSSP must perform this activity. This is the act of conducting correlation of open and closed source research into exploits or threat-based activities observed on commercial, open source, internal, or provisioned mission owner networks to validate and investigate indicators. While the CSSP is accountable, the CSP will need to provide supporting information.

1. The CSSP will:

a. Aggregate all information from the CSP and correlate that information with intelligence information received through intelligence community channels within the DoD.

b. Support DODIN operations and DCO internal defensive measures by providing ongoing awareness and security status of an organization's security posture and reportable cyber events and incidents.

c. Support timely informed and actionable cyber incident handling decisions in accordance with Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01.

d. Maintain ongoing community awareness and security status of reportable cyber events and incidents to support timely, informed, and actionable cyber incident handling decisions.

e. Support timely, informed, and actionable risk decisions and continued risk management framework decisions.

2. The CSP will:

a. Conduct correlation of open and closed source research into exploits or malware.

b. Conduct correlation of available data sources to validate and investigate indicators.

c. Correlate the data from the original indicator, with all other available data sets to support or refute the indication of malicious activity.

d. Define passive attribution within the capabilities of the available indicators, with attribution defined as the correlation between an internet protocol address; domain; TTPs, or other indicators to associate activity to tracked intrusion sets or nation state activity if warranted.

e. Conduct de-confliction activities through trusted agents if that DCRT or exercise related activity is suspected but unconfirmed.

(c) Malware Notification. The CSSP must perform malware notification. The CSSP will alert mission owners to new malware and assists the mission owner when an incident occurs.

1. The CSSP will:

a. Maintain contact with anti-malware software vendors so that effective countermeasures are developed, tested, and deployed as quickly as possible.

b. Notify the mission owner of all potential malware threats.

2. The CSP will report any findings or related events to the CSSP.

(3) Detection Processes. The CSSP will maintain and test detection processes and procedures to ensure awareness of anomalous events.

(a) Network Security Monitoring and Intrusion Detection for BCP Functions. This is a DoD-performed activity, which must be performed by the CSSP, since BCP monitors ingress and egress points to commercial CSP environments of the Defense Information Systems Network to detect and report unauthorized activity and determine if network and host activity is intrusion related. This involves vertical and horizontal information sharing internal to the DoD on classified networks using classified channels. Due to the traffic in IL2, IL2 CSO is not required to pass through the Internet Access Point or Boundary Cloud Access Points per the DoD Cloud Computing Security Requirements Guide.

(b) Network and Endpoint Security Monitoring at the Enclave Level. A DoD entity or commercial entity can perform this activity to detect unauthorized activity by monitoring access to the host. The DoD or commercial entity performing network and endpoint security monitoring at the enclave level will:

1. Monitor the mission owner's environment 24/7/365.
2. Report anomalous events detected to the mission owner and the CSSP.
3. Provide copies of audit and system logs as requested by the CSSP POC for correlation activities and requirements from USCYBERCOM and/or JFHQ-DODIN.
4. Correlate vulnerability management data with network and endpoint security monitoring to provide fewer false positives, a higher level of fidelity for incident detection, handling, and countermeasure.
5. Track and execute corrective actions.
6. Report actions to the mission owner and the CSSP.
7. Support incident reporting activities by providing event information to the mission owner and CSSP within the timelines identified in CJCSM 6510.01. For IaaS and PaaS, if the CSSP has the technical capability to leverage intel-derived signatures specific to the DoD, then the activity must be performed by a CSSP.

(4) DODIN User Activity Monitoring (UAM) for the DoD Insider Threat Program. A DoD or commercial entity must perform DODIN UAM. The implementation and capability can be performed by a CSSP or outsourced. This refers specifically to the portion where the DoD workforce is operating, which does not include the CSP infrastructure. Before deciding to outsource any aspect of the UAM, the authorizing official will ensure that the DoD Component legal advisor reviews the provider's ability to legally perform UAM functions.

(a) Employ UAM Capabilities to Detect Anomalous Insider Activity. Outsourcing guidance varies by service model and IL (see Table 1 for more information.) The

implementation and actions to detect anomalous activity can be performed by a DoD entity or commercial entity, in coordination with the CSSP, depending on the risk that the authorizing official deems appropriate and in accordance with DoDD 5205.16.

1. The entity employing UAM capabilities to detect anomalous insider user activity will:

a. Document UAM procedures and share them with the mission owner.

b. Implement capabilities and procedures to respond to anomalous user activity on the mission owner's environment, including procedures to mitigate potential damage to data on the mission owner's environment and report activity to the mission owner and the CSSP.

c. Provide a detailed report, track, execute corrective actions, as appropriate, and report actions to the mission owner and the CSSP POC.

d. Share collected data with the mission owner and the CSSP by means specified by the mission owner.

2. The DoD entity will:

a. Coordinate with the DoD Component insider threat organization to provide system indicators that could inform an insider threat investigation.

b. Ensure training for all analysts to coordinate with insider threat and law enforcement (LE).

(b) Maintain Insider Threat Audit Data. A DoD entity or commercial entity can perform this activity. The entity maintaining insider threat audit data will:

1. Implement procedures to maintain audit data and preserve audit data chain of custody.

2. Secure data collected to support insider threat in compliance with applicable Federal and DoD regulations.

3. Document all procedures for chain of custody of UAM data and share with mission owner.

(c) Correlate Insider Threat Audit Data with Threat Data. This must be performed by a DoD entity, who will:

1. Coordinate with LE and counterintelligence element to correlate insider threat profiles.

2. Acknowledge, maintain, and reference any trend analysis to identify common vulnerabilities, and develop countermeasures and mitigation strategies or remediation.

(5) Cyber Protection Condition (CPCON) and Orders (e.g., TASKORD, Operational Order (OPORD), Fragmentary Order.

(a) CPCON and Orders Implementation. A DoD entity or commercial entity can perform this activity. The entity performing CPCON and orders implementation will:

1. Execute approved CPCON level and DoD orders actions specified by the mission owner or the CSSP.
2. Share operational and technical impacts of any change or execution of a DoD order and a tailored readiness option with the mission owner and CSSP by means specified by the mission owner, in accordance with USCYBERCOM Instruction 5200-13.
3. Keep the mission owner and CSSP apprised to the status of implementation as requested.

(b) CPCON and Orders Notification and Assistance. A CSSP must perform this activity.

1. The mission owner will:
 - a. In accordance with JFHQ-DODIN OPORD 17-0217, the mission owner must report compliance of executed DoD order and CPCON level actions and coordinate with the CSSP on any issues.
 - b. In coordination with the CSSP, prioritize and disseminate information and requirements to the CSP as required.

2. The CSSP will:
 - a. Notify mission owner of any CPCON changes or orders.
 - b. Monitor the mission owner's compliance with the order.
 - c. Provide technical subject matter expertise support to the mission owner upon request.

d. Respond. These activities are conducted to respond to, contain, and mitigate a detected cybersecurity event or incident.

(1) Incident Categorization. This activity must be performed by the CSSP, who will declare the category and severity of the incident or event. All information gathered will conform to the existing incident criteria in accordance with DoDI 8530.03, and corresponding timelines identified in CJCSM 6510.01.

(2) Incident Reporting. The CSSP must perform this activity because only CSSPs have access to the classified incident reporting system and access to the classified information channels for disseminating and reporting incidents and events in accordance with JFHQ-DODIN OPORD 17-0217 or succeeding orders. The CSSP will perform incident reporting in accordance with DoDI 8530.03. The mission owner must direct compliance by the CSP in any agreement and identify the CSSP responsible for incident reporting in the system/network approval process database.

(a) The CSP will support the CSSP by:

1. Implementing procedures to support the CSSP to conduct incident handling in accordance with applicable DoD guidance, categorization, and timelines.

2. Reporting events under investigation and all potential incidents and correlated information from these incidents and events that occur on mission owner systems using documented procedures.

3. Providing event and incident artifacts to the mission owner and the CSSP, who will report those using secure internal DoD systems to USCYBERCOM.

4. Safeguarding and delivering all information related to incidents upon request from the identified CSSP for LE and counterintelligence requirements.

(b) The CSSP will enter incidents into the secure internal DoD systems to USCYBERCOM on behalf of the mission owner.

(3) Incident Handling Response. A DoD entity or commercial entity can perform this activity. Implementation procedures and timing will be decided by the CSSP and the mission owner. The entity performing incident handling response will:

(a) Perform incident response activities in accordance with the DoD Cloud Computing Security Requirements Guide, DoDI 5200.48, and Subpart 204.73 of the Defense Federal Acquisition Regulation Supplement (DFARS).

(b) Provide a portfolio of offerings that can perform volatile data analysis, forensic media analysis, or reverse engineering and malware analysis from suspected compromised systems or files.

(c) Perform a damage assessment or incident response analysis and report it to the mission owner and CSSP.

(d) Acknowledge, maintain, and reference all trend analysis or post-incident analysis disseminated by the CSSP or mission owner.

(e) Provide any applicable follow-up and timely feedback to post-incident analysis.

(f) Develop countermeasures and mitigation strategies or remediation that are recommended for approval to the CSSP.

(g) Track and execute corrective actions as appropriate and report actions to the mission owner and the CSSP.

(4) Incident Response –LE. The CSSP must perform this activity. In accordance with Subpart 204.73 of the DFARS, DoD Component heads will ensure that they share cyberspace incident-related investigative, LE, and operational information with the CDRUSCYBERCOM and Director, Defense Counterintelligence and Security Agency, for cleared defense contractors.

(a) The CSSP will:

1. Acquire and preserve copies of digital media, logs, and investigative and technical data associated with cyber intrusion incidents and investigations.

2. Using predefined agreements and TTPs with the mission owner, notify the DoD LE agencies responsible for the affected portion of the DODIN of cyber mission forces (CMF) deployment, and any LE support requested.

(b) The mission owner will:

1. Comply with appropriate policy guidance for LE and criminal investigations that relate to cyberspace.

2. Notify DoD LE agencies responsible for the affected portion of the DODIN of CMF deployment, and any LE support requested.

3. Ensure that the DoD Component heads respective LE communities share cyberspace incident-related investigative, counterintelligence element, and operational information with the CDRUSCYBERCOM and Director, Defense Counterintelligence and Security Agency, for cleared defense contractors.

(c) The CSP will coordinate with the CSSP to acquire and preserve copies of digital media, logs, and investigative and technical data associated with cyber intrusion incidents, investigations, and operations.

(5) Incident Response – Counterintelligence. The CSSP must perform this activity. In accordance with DoD Manual 8530.01, DoD Component heads will ensure they share cyberspace incident-related investigative, counterintelligence element, and operational information with the CDRUSCYBERCOM and Director, Defense Counterintelligence and Security Agency, for cleared defense contractors. Military Department counterintelligence element communities will coordinate with the CDRUSCYBERCOM and Director, Defense Counterintelligence and Security Agency, as appropriate, regarding investigation versus protection cost-benefit decisions to minimize negative impacts to investigations and operations.

(a) The CSSP will:

1. Acquire and preserve copies of digital media, logs, and investigative and technical data associated with cyber intrusion incidents, investigations, and operations in accordance with DoDD 5106.01.

2. Using predefined agreements and TTPs with the mission owner, notify the DoD counterintelligence element responsible for the affected portion of the DODIN of CMF deployment, and any counterintelligence element support requested.

(b) In coordination with the CSSP, the mission owner will ensure that their respective DoD Component's counterintelligence element share cyberspace incident-related investigative, counterintelligence element, and operational information with the CDRUSCYBERCOM and Director, Defense Counterintelligence and Security Agency, for cleared defense contractors.

(c) In coordination with the CSSP, the CSP will acquire and preserve copies of digital media, logs, and investigative and technical data associated with cyber intrusion incidents, investigations, and operations in accordance with DoDD 5106.01.

(6) Incident Response – Analysis. The CSSP must perform this activity. This activity can consist of volatile data analysis, forensic media analysis, reverse engineering/malware analysis, and intrusion assessments. There is a shared responsibility to provide information between the CSP and CSSP. The CSP must make the data available to the CSSP consistent with the incident event category, nature, and severity of impact in accordance with DoDI 8530.03.

(a) The CSSP will:

1. Provide the capability to analyze and respond to events or cyber incidents to mitigate any adverse operational or technical impact on the DoD Component-owned or -operated portion of the DODIN in accordance with DoDIs 8530.03, 8582.01, and DoDD 5106.01.

2. Provide the capability to determine the current adequacy of cybersecurity measures for the DoD Component portion of the DODIN; identify deficiencies; provide data from which to predict the effectiveness of proposed cybersecurity measures; and confirm the adequacy of such measures after implementation.

3. Acquire and preserve copies of digital media, logs, and investigative and technical data associated with cyber intrusion incidents, investigations, and operations required for tactical analysis, strategic analysis, or LE investigations in accordance with DoDD 5106.01.

4. Report findings into the DoD Cyber Incident Management System in accordance with CJCSM 6510.01.

5. Record any lessons learned in the Joint Lessons Learned Information Systems.

(b) The mission owner will:

1. Deliver required CSP incident response artifacts to the CSSP.
2. Specify the CSSP as the cybersecurity POC in all documentation and coordination with the CSP to allow simultaneously sharing of cyber information between the CSP and CSSP.
3. Ensure the assigned cyber protection team reports to the CSSP to coordinate all incident response activities.
4. Verify, validate, and articulate the operational impact on incidents and report to the CSSP.

(c) The CSP will:

1. Implement passive countermeasures where feasible and notify the mission owner and the CSSP.
2. Retain all incident artifacts and documentation in accordance with the approved records disposition schedule for the applicable DoD Components pursuant to Subpart 1222.32 of Title 36, Code of Federal Regulations. Collected data will be shared with the mission owner and the CSSP via means specified by the CSSP, upon request in accordance with Subpart 204.73 of the DFARS.

GLOSSARYPART I. ABBREVIATIONS AND ACRONYMS

ACRONYM	MEANING
AS&W	attack sensing and warning
BCP	boundary cyberspace protection
CDRUSCYBERCOM	Commander, United States Cyber Command
CJCSM	Chairman of the Joint Chiefs of Staff manual
CMF	cyber mission forces
CPCON	cyber protection condition
CSO	cloud service offering
CSP	cloud service provider
CSSP	cybersecurity service provider
DCAT	DoD Cyber Assessment Team
DCO	defensive cyberspace operations
DCRT	DoD Cyber Red Team
DFARS	Defense Federal Acquisition Regulation Supplement
DoD CIO	DoD Chief Information Officer
DoDD	DoD directive
DoDI	DoD instruction
DODIN	Department of Defense information network
DTM	directive-type memorandum
EVS	external vulnerability scan
FedRAMP	Federal Risk and Authorization Management Program
IaaS	infrastructure as a service
IL	impact level
ISCM	information security continuous monitoring
JFHQ-DODIN	Joint Force Headquarters-Department of Defense Information Network
LE	law enforcement
OPORD	operational order
PaaS	platform as a service
PM	program manager
POC	point of contact

ACRONYM	MEANING
SaaS	software as a service
SP	special publication
TASKORD	tasking order
TTP	tactics, techniques, and procedures
UAM	user activity monitoring
USCYBERCOM	United States Cyber Command
VAA	vulnerability assessment and analysis
WVS	web vulnerability scan

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this DTM.

TERM	DEFINITION
authorizing official	Defined in Office of Management and Budget Circular A-130.
commercial entity	A CSP or contracted provider by the DoD Component authorizing official authorizes to provide cybersecurity activities (the cognizant mission owner retains responsibility for performance).
CSP	The on-site hosting entity, off-premise hosting entity, or a third party entity offering CSOs.
CSSP	A DoD organization that USCYBERCOM authorizes to perform one or more of the cybersecurity activities, internally (on behalf of the DoD Component) or externally, (as a CSSP providing cybersecurity services to a DoD Component).
DoD entity	A DoD Component authorized to perform one or more CSSP services internally or externally on behalf of their own Component.
DoD sponsor	The organization that will complete or assist the commercial entity with completing the appropriate authorization package.
IL 2	Defined in the DoD Cloud Computing Security Requirements Guide.
IL 4	Defined in the DoD Cloud Computing Security Requirements Guide.

TERM	DEFINITION
IL 5	Defined in the DoD Cloud Computing Security Requirements Guide.
IL 6	Defined in the DoD Cloud Computing Security Requirements Guide.
mission owner	A DoD “cloud consumer” as defined in National Institute of Standards and Technology Special Publication 500-292.