DEPARTMENT OF WAR
6000 Defense Pentagon
Washington, D.C. 20301-6000

CHIEF INFORMATION OFFICER

July 28, 2026

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
DEFENSE AGENCY AND DOW FIELD ACTIVITY DIRECTORS

SUBJECT: Directive-type Memorandum 26-003 – "Cybersecurity Service Provider Definition Clarification"

References: See Attachment 1.

Purpose. In accordance with the authority in DoD Directive 5144.02, this directive-type memorandum (DTM) establishes policy, assigns responsibilities, and provides procedures for:

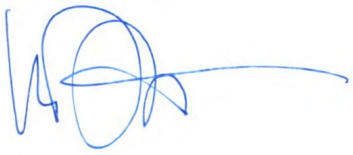
- The minimum baseline requirements to be certified and authorized as a DoW cybersecurity service provider (CSSP).
- The requirements that outline the systems, networks, and information that require alignment to a CSSP.
- Who performs the authorization and certification of DoW CSSPs.
- Is effective July 28, 2026; it will be incorporated into DoD Instruction (DoDI) 8530.01. This DTM will expire effective July 28, 2028.

Applicability. This DTM applies to OSW, 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 War, the Defense Agencies, the DoW Field Activities, and all other organizational entities within the DoW (referred to collectively in this DTM as the "DoW Components").

Definitions. See Glossary.

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/.



Kirsten A. Davies
DoW Chief Information Officer

Attachments:
As stated

ATTACHMENT 1

REFERENCES

Chairman Joint Chiefs of Staff Manual 6510.01, "Cyber Incident Handling Program," July 10, 2012

Committee on National Security Systems Instruction 1010, "Cyber Incident Response," September 27, 2021

Committee on National Security Systems Instruction 4009, "Committee on National Security Systems (CNSS) Glossary," April 6, 2015

Defense Federal Acquisition Regulation Supplement, Subpart 204.73, current edition

Directive-type Memorandum 24-001, "DoD Cybersecurity Activities Performed for Cloud Service Offerings," February 27, 2024, as amended

DoD Cyber Exchange, "Network Infrastructure Policy Security Technical Implementation Guide," current edition[1]

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 Instruction 4000.19, "Support Agreements," December 16, 2020

DoD Instruction 5205.16, "The DoD Insider Threat Program," December 20, 2024

DoD Instruction 8110.01, "Mission Partner Environment Information Sharing Capability Implementation for the DoD," June 30, 2021

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

DoD Manual 5400.11, Volume 2, "DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan," May 6, 2021, as amended

DoD Manual 8530.01, "Cybersecurity Activities Support Procedures," May 31, 2023

DoW Instruction 5015.02, "DoW Records Management Program," June 26, 2026

Federal Acquisition Regulation, current edition

Intelligence Community Directive 502, "Integrated Defense of the Intelligence Community Information Environment," March 11, 2011

Intelligence Community Directive 503, "Intelligence Community Information Environment Risk Management," October 25, 2024

[1] Available at https://cyber.mil/stigs/

Intelligence Community Standard 500-27, "(U) Collection and Sharing of Audit Data," June 2, 2011[2]

Intelligence Community Standard 700-2, "Use of Audit Data for Insider Threat Detection," June 2, 2011[2]

International Organization for Standardization and International Electrotechnical Commission 27039:2015, "Information technology — Security Techniques — Selection, Deployment and Operations of Intrusion Detection and Prevention Systems (IDPS)," February 2015[3]

Joint Forces Headquarters-Department of Defense Information Network (USCYBERCOM) Campaign Order 24-0052 (8600-26), "Directing DODIN Operations and Defensive Cyber Operations-Internal Defensive Measures (DCOIDM)," November 7, 2025[4]

Joint Publication 6-0, "Joint Communications," December 4, 2023[5]

Manual for Courts-Martial, United States, current edition

National Institute of Standards and Technology Interagency or Internal Report 8286 Rev. 1, "Integrating Cybersecurity and Enterprise Risk Management (ERM)," December 2025[6]

National Institute of Standards and Technology Special Publication 800-150, "Guide to Cyber Threat Information Sharing," October 2016[7]

Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition

United States Code, Title 10, Chapter 47

United States Cyber Command Instruction 5200-13, "Cyber Protection Conditions," April 13, 2019[8]

[2] To request a copy, email: NITTF@odni.gov

[3] Available at: https://standards.iteh.ai/catalog/standards/sist/e091454d-a229-428b-8d39-9280a8612e99/iso-iec-27039-2015

[4] To request a copy, email: dcdc.meade.j3.mbx.j35-opord-8600@mail.smil.mil

[5] Available at: https://jdeis.js.mil/jdeis/index.jsp?pindex=27&pubId=964

[6] Available at: https://csrc.nist.gov/pubs/ir/8286/r1/final.

[7] Available at: https://doi.org/10.6028/NIST.SP.800-150.

[8] Available at: https://intelshare.intelink.gov/sites/jfhq-dodin/JD/Shared%20Documents/Inspection%20Programs/CSSP/Useful%20Documents/USCCI%205200-13%20CPCON.pdf#search=5200%2D13

ATTACHMENT 2

RESPONSIBILITIES

1. DOW CHIEF INFORMATION OFFICER (DOW CIO). The DoW CIO:

a. Approves or disapproves all CSSP certification requests and sends all approvals to the Commander, United States Cyber Command (CDRUSCYBERCOM) or their designee.

b. Is the authorizing official (AO) for special access program (SAP) systems not processing sensitive compartmented information (SCI).

c. Adjudicates CSSP certification appeals with the United States Cyber Command (USCYBERCOM).

2. DIRECTOR, DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY (DCSA). Under the authority, direction, and control of the Under Secretary of War for Intelligence and Security and in addition to the responsibilities in Paragraph 3 of this attachment, the Director, DCSA coordinates with the Secretaries of the Military Departments and the CDRUSCYBERCOM regarding investigation versus protection cost-benefit decisions to minimize negative impacts to investigations and operations, as appropriate.

3. DOW COMPONENT HEADS. The DoW Component heads:

a. Align to a CSSP and direct network operations and cybersecurity activities or authorized CSSPs for cybersecurity services in accordance with DoD Manual (DoDM) 8530.01.

b. Ensure information sharing requirements of Subpart 204.73 of the Defense Federal Acquisition Regulation Supplement are met with Director, DCSA and CDRUSCYBERCOM.

c. Ensure records and information established and created in accordance with this issuance are retained in accordance with DoW Instruction 5015.02 and DoW Component records management disposition schedules.

d. In accordance with DoDI 4000.19, ensure support agreements governing CSSP operations adhere to standardized processes and reviews that delineate roles and responsibilities.

4. SECRETARIES OF THE MILITARY DEPARTMENTS. In addition to the responsibilities in Paragraph 3 of this attachment, the Secretaries of the Military Departments coordinate with the CDRUSCYBERCOM and the Director, Defense Counterintelligence and Security Agency regarding investigation versus protection cost-benefit decisions to minimize negative impacts to investigations and operations, as appropriate.

5. CDRUSCYBERCOM. The CDRUSCYBERCOM performs the duties in Paragraph 3 of this attachment and:

a. Implements the general service (GENSER) DoW CSSP processes in coordination with and approved by the DoW CIO and the SAP AO for GENSER-level SAP programs. Functions as the certifier for GENSER and SAP TOP SECRET (TS) Collateral and below and as the AO for GENSER TS Collateral and below.

b. Maintains the evaluator scoring metrics in coordination with the CSSP community and guidance from the DoW CIO Chief Information Security Officer and the DoW SAP AO for GENSER only SAPs.

ATTACHMENT 3

CSSPS

1. CSSP ACTIVITIES.

a. Some cybersecurity activities are inherently governmental functions that must be performed by, or under the oversight and responsibility of, a DoW Component head. The performance of all cybersecurity activities includes reporting to and collaboration with the aligned CSSP. A CSSP is designated by a DoW Component head and must continuously monitor to detect, analyze, and respond to anomalous, suspicious, or malicious activities on DoW cyber terrain.

(1) CSSPs have personnel and resources to triage time-sensitive events or incidents, and initiate response actions based on severity and event or incident categorization. Incidents must be reported when the incident categorization has occurred. At maximum, CSSPs have 72 hours to triage, and 24 hours to provide an incident report to USCYBERCOM and Department of Defense Cyber Crime Center (for Defense Industrial Base incidents) as directed by Chairman Joint Chiefs of Staff Manual (CJCSM) 6510.01. Incidents indicating that personally identifiable information has been improperly accessed or transferred, require reporting in accordance with DoDI 8530.03 and Volume 2 of DoDM 5400.11.

(2) DoW CSSPs must maintain a valid certification in accordance with the procedures outlined in Paragraph 4 of this attachment and an authorization to operate (ATO) as described in Paragraph 5 of this attachment. Failure to maintain a valid certification and ATO will result in the suspension of CSSP services.

(3) Information on CSSP certification standards can be found in DoDM 8530.01.

b. CSSPs can pursue all activities in DoDI 8530.01 but must perform the cybersecurity activities in Attachment 4 of this DTM and referenced in the CSSP Minimum Cybersecurity Activities Checklist found at https://cybersecurityks.osd.mil/kscollaboration/CSSP/Pages/CSSPCSActivities.aspx to be certified and authorized as a DoW CSSP. The DoW Component head must ensure compliance of all cybersecurity activities outlined in DoDM 8530.01.

2. CSSP Alignment.

The requirement to align to a CSSP and comply with DoDM 8530.01 activities also applies to all cloud instances in DTM 24-001 and all coalition or mission partner environments, SAPs, and intelligence networks. Likewise, this requirement applies to all technology/capabilities within the DoW, including industrial controls, internet of things, operational technology, artificial intelligence systems, and quantum computers/networks. This requirement to align to a CSSP cannot be waived or risk accepted when AOs authorize systems, regardless of network, connectivity, or mission.

3. CYBERSECURITY AND CYBER DEFENSE SHARED RESPONSIBILITIES.

a. DoW Component heads bear ultimate responsibility for the cybersecurity of all systems and networks under their control.

b. Cyber defense relies on engineers, mission owners, and local defenders (government or contracted) that have direct access to the information, networks, and systems being defended. Information system security officers (ISSOs) and information system security managers (ISSMs) ensure that they coordinate and deconflict with a CSSP for all cybersecurity activities in accordance with DoDI 8530.01 and assist when requested by their certified CSSPs.

4. CSSP CERTIFICATION.

a. In accordance with DoDI 8530.01, DoW Components can request to become certified CSSPs. The request to certify a CSSP includes the package and all supporting artifacts and will be sent to the DoW CIO at osd.pentagon.dod-cio.mbx.dod-cio-cssp@mail.mil. The application package submission process and necessary contents are outlined in DoDM 8530.01.

b. Once approved by the DoW CIO, the DoW CIO sends the submission to USCYBERCOM, or its designee, to review and add to the certification schedule.

(1) For renewal of an existing CSSP certification, the package and supporting artifacts are submitted to USCYBERCOM (USCC_J361_SOD_Integration@nsa.gov) and certification results and authorizations to operate are forwarded to the DoW CIO to confirm continued compliance with DoDI 8530.01 requirements.

(2) For CSSP organizations, the CSSP lead can submit appeals of findings meeting DoDI 8530.01 requirements to the DoW CIO (osd.pentagon.dod-cio.mbx.dod-cio-cssp@mail.mil) and USCYBERCOM (USCC_J361_SOD_Integration@nsa.gov) within 5 days of receiving the certification findings. Final outcome and adjudication of the finding, along with the original certification information, will be included in the ATO package.

c. In accordance with Intelligence Community (IC) Directives (ICDs) 502 and 503, IC Components within the DoW must:

(1) Ensure assessments for CSSP capabilities comply with SCI systems, networks, and applications in accordance with ICDs 502 and 503.

(2) Maintain assessment criteria aligned with DoDI 8500.01, and the objectives in IC Standards 500-27 and 700-2 as they relate to insider threat detection and response.

5. AO FOR CSSP ACCREDITATIONS.

a. For SAPs that do not process SCI, the DoW CIO serves as the AO.

b. For GENSER information systems operating at the TS Collateral and below classification level, the CDRUSCYBERCOM serves as the AO.

c. The Director of National Intelligence is responsible for ensuring that each IC element within the DoW functions as the AO for its own systems processing TS-SCI, in accordance with the authority granted by ICD 503 and the requirements in ICD 502.

ATTACHMENT 4

CSSP MINIMUM CYBERSECURITY ACTIVITIES

1. CORRELATE ASSET AND VULNERABILITY DATA WITH THREAT DATA. CSSPs conduct open-source vulnerability research and establish correlation processes utilizing subscriber-provided asset data to identify exploits or threat actor opportunities.

a. The CSSP:

(1) Aggregates all asset and vulnerability information and correlates that information with cyber threat intelligence information received through intelligence community channels within the DoW.

(2) Analyzes correlated asset, threat, and vulnerability data to determine probability and impact of vulnerability; assesses the overall security posture of assets, and shares information with the Commander, Department of Defense Cyber Defense Command (DCDC); aligned DoW Component head; other CSSPs; and ISSOs or ISSMs.

b. The ISSO or ISSM:

(1) In conjunction with the CSSP, assesses the data from the originally provided indicator, with all other available data, to determine the likelihood of exploitation and supports or refutes the indication of malicious activity within the environment, system, or program of record.

(2) Defines passive attribution within the capabilities of any available indicators.

(3) Utilizes correlated and analyzed asset, threat, and vulnerability data from the CSSP to identify and prioritize remediation or mitigation actions to improve the security posture.

2. MALWARE NOTIFICATION.

a. The CSSP:

(1) Conducts malware reporting notifications in accordance with DoDI 8530.01, DoDM 8530.01, and CJCSM 6510.01.

(2) Confirms subscribers or mission/system owners acknowledge notification.

b. ISSOs or ISSMs must report any malware findings or related events to the AO, the information owners, and the CSSP.

3. DETECTION PROCESSES.

a. The CSSP will perform cybersecurity monitoring activities to detect unauthorized activity and anomalous events.

b. The CSSP will perform detection at multiple architectural layers to achieve the necessary visibility over Department of Defense information network (DoDIN) resources and data.

c. Roles and responsibilities for entities performing detection processes must be clearly documented, fully understood, and effectively executed by all parties.

d. Data sharing among responsible entities and the aligned CSSP is required to enable full effectiveness for detection processes and activities. This activity is split into multiple segments of the architecture.

e. There are three locations of the architecture that must be addressed, commonly referred to as "tiers" in accordance with CJCSM 6510.01. Network Tiers 1-3 are defined in Paragraphs 3.e.(1)-(3) of this attachment.

(1) Tier 1: Network Security Monitoring and Intrusion Detection for Internet Access Point (IAP) or Boundary Cloud Access Point (BCAP) Functions.

(a) Tier 1 represents the outermost security layer of the network architecture, encompassing network security monitoring and intrusion detection for IAPs and BCAPs. These functions provide the initial point of entry for external connections and peering points between external networks and the DoDIN. Tier 1 entities will maintain continuous, 24/7 monitoring of all ingress and egress traffic to detect and report unauthorized activity. If a DoW Component head operates an IAP or BCAP, a designated DoW cybersecurity entity will perform this monitoring activity.

(b) Tier 1 activities will not be evaluated or certified as part of the standard CSSP process. Tier 1 operations are distinct from traditional CSSP functions. Because the evaluator scoring metrics are designed specifically to assess defensive cyber operations within enclaves and internal perimeter networks, they do not include the specialized requirements associated with IAP or BCAP functions.

(2) Tier 2: Network Security Monitoring and Intrusion Detection for Enclave/Perimeter Functions.

(a) Tier 2 is the middle tier and is the perimeter or enclave boundary within the architecture. This is commonly the tier referred to when discussing CSSP defense of ingress and egress at the point of presence for local networks.

(b) This activity is in accordance with the Network Infrastructure Policy Security Technical Implementation Guide and must be performed by a DoW CSSP on a 24/7 basis to monitor ingress and egress points at physical (e.g., command communications service designator) or virtual (e.g., software-defined, user-defined) perimeters that represent point of presence between DoW Component head internal network and access to the internet, another enclave, or to an edge router. The CSSP:

1. Monitors ingress and egress to the local network environment 24/7 for anomalous and malicious activity. Monitoring can be performed utilizing automated

technologies to offset the cost of personnel; however, this must be proven to be efficient during the evaluation process.

2. Correlates and analyzes detected events with associated audit data to identify cyber incidents; when required, initiates incident handling activities.

3. Tracks and executes corrective actions in coordination with ISSOs or ISSMs.

4. Maintains and tests detection processes and procedures to ensure awareness of anomalous events.

5. Performs incident reporting activities by providing event information to the ISSOs or ISSMs, the AO, and the Commander, DCDC within the timelines identified in CJCSM 6510.01.

6. If the CSSP detects anomalous egress activity, it may indicate that personally identifiable information has been improperly accessed or transferred and incident details must then be reported in accordance with DoDI 8530.03 and Volume 2 of DoDM 5400.11.

(3) Tier 3: Internal Network and Security Monitoring.

(a) Tier 3 is the local network that ISSOs or ISSMs focus on. The AO must ensure protections for their respective oversight for each layer of defense.

(b) A DoW entity or commercial entity can perform this activity to detect unauthorized activity by monitoring access to the host. For network and endpoint security monitoring:

1. The CSSP:

a. Collects all information provided by the ISSO or ISSM.

b. Correlates received information with existing threat posture.

c. Reports any findings to the AO, the ISSO, or the ISSM, and information owners.

d. Shares any new findings with other CSSPs.

2. The ISSOs or ISSMs:

a. Monitor the internal local network 24/7. Monitoring can be performed utilizing automated technologies to offset the cost of personnel.

b. Share documented normal behavior (including data flow, ports, protocols, and services, and network connection diagrams) that detail how the

system or network normally operate and provide that information to the AO, the CSSP, and the information owners.

c. Report anomalous events detected to the AO, the CSSP, and the information owners.

d. Share copies of audit and system logs as requested by the CSSP point of contact for correlation activities and requirements from USCYBERCOM and/or DCDC.

e. Correlate vulnerability management data with network and endpoint security monitoring to provide fewer false positives and a higher level of fidelity for incident detection, handling, and countermeasures.

f. Track and execute corrective actions.

g. Report and provide event information to the AO, the CSSP, and the information owners within the timelines identified in accordance with CJCSM 6510.01 and DoDI 8530.03.

4. ORDERS, CYBER PROTECTION CONDITION (CPCON), AND ASSISTANCE.

a. Orders. Implementing orders is a shared responsibility between entities (e.g., CSSP, DoW cybersecurity entity, commercial entity). Each order may require unique implementation by one or more entities to achieve complete order compliance. A CSSP must assist subscribers, when requested, for any orders that fall within the CSSP areas of expertise. The role of CSSPs in the orders implementation processes and the requirements for other responsible entities to collaborate with aligned CSSPs when implementing orders are described in Paragraphs 4.a.(1)-(3) of this attachment.

(1) Orders Notification. The CSSP entity performing orders notification:

(a) Receives and evaluates orders for applicability and task association.

(b) Prioritizes and disseminates information and requirements, with supplemental guidance, if necessary, to appropriate personnel for implementation.

(c) Tracks and reports compliance with DoW orders actions in accordance with defined reporting requirements.

(2) Orders Assistance. The CSSP must:

(a) Provide technical subject matter expertise support to the AOs, the ISSOs, the ISSMs, and the information owners upon request.

(b) Evaluate potential technical and operational impacts from execution of a DoW order and communicate impacts with the entity issuing the order, the AO, the ISSOs, the ISSMs, and the information owners as appropriate.

(c) Keep the entity issuing the order, the AO, the ISSOs, the ISSMs, and the information owners apprised of the status of implementation, as appropriate.

(3) Orders Implementation.

(a) The CSSP:

1. Executes and provides guidance and recommendations for the actions specified in the orders.

2. Keeps the entity issuing the order, the AO, the ISSOs, the ISSMs, and the information owners apprised of the status of implementation, as appropriate.

(b) ISSOs or ISSMs:

1. Evaluate potential technical and operational impacts from execution of a DoW order and communicate impacts with the entity issuing the order, the AO, the CSSP, and the information owners, as appropriate.

2. Keep the entity issuing the order, the AO, the CSSP, and the information owners apprised of the status of implementation, as appropriate.

3. Share operational and technical impacts of any change or execution of a DoW order and a tailored readiness option with the AO, the CSSP, and the information owners by means specified in accordance with USCYBERCOM Instruction 5200- 13.

b. CPCON. In addition to all actions in Paragraphs 4.a.(1)-(3), a CSSP:

(1) Prioritizes CSSP-owned capabilities, assets, and supporting systems based on criticality (i.e., mission critical, mission essential, mission support, and non-essential).

(2) Provides prioritized capabilities, assets, and supporting system information to the DCDC and the AO.

(3) Maintains copies of the latest CPCON procedures and provides copies of local procedures to DCDC and the AO.

5. CYBER INCIDENT HANDLING, CATEGORIZATION, AND REPORTING.

a. Incident Handling.

(1) Combatant Commands, Military Services, Defense Agencies, and DoW Field Activities are responsible for protecting their networks, and each organization has a unique mission set across the DoW.

(a) These organizations must execute defensive cyber operation – internal defensive measure activities to protect their own networks and protect the gateway point of entry to the DoDIN, both classified and unclassified terrains, including incident handling and reporting in accordance with DoDIs 8530.01 and 8530.03 and DCDC Campaign Order 24-0052 (8600-26).

(b) The DoW Component head is accountable for how their organization responds to a cyber incident or event, and their designated cybersecurity entities must be prepared to immediately isolate and neutralize a threat, whether internal or external.

(2) DoW cybersecurity entities must understand the organizational lines of operation and responsibilities aligned to the organizational mission set when executing their responsibilities for cyber incident handling. The roles and responsibilities for cyber incident handling activities that must be performed by a certified DoW CSSP include:

(a) Incident categorization.

(b) Incident reporting.

(c) Incident handling response coordination with law enforcement (LE) or counterintelligence (CI).

(d) Incident analysis.

(e) The CSSP categorizes all cyber incidents in accordance with CJCSM 6510.01, which identifies incident categories and their associated reporting timelines.

b. Incident Reporting.

(1) The CSSP:

(a) Performs incident reporting in accordance with DCDC Campaign Order 24-0052 (8600-26) or succeeding orders; CJCSM 6510.01B; and DoDM 8530.01.

(b) Enters incidents into the secure internal DoW systems to the USCYBERCOM and/or the DoW Cyber Crime Center on behalf of the ISSO or ISSM.

(c) Shares all incident data with the AO.

(2) The ISSO or ISSM:

(a) Supports the CSSP to conduct incident handling in accordance with applicable DoW guidance, categorization, and timelines.

(b) Reports events under investigation and all potential incidents and correlated information from these incidents and events that occur on systems using documented procedures.

(c) Provides event and incident artifacts to the CSSP, who will report those to the USCYBERCOM and the DoW Cyber Crime Center using secure internal DoW systems.

(d) Safeguards and delivers all information related to incidents upon request from the identified CSSP for LE and CI requirements.

6. LE/CI.

a. Due to the sensitivity and criticality of LE/CI investigations of compromised systems, the CSSP may leverage existing LE/CI established liaisons to conduct forensic investigations of compromised systems and defer to their established processes and authorities upon declaration of intent by the cognizant organization in the conduct of their investigations.

b. The CSSP:

(1) Acquires, preserves, and documents copies of digital media, logs, and investigative and technical data associated with cyber intrusion incidents and investigations in accordance with organization/LE documented chain of custody procedures in accordance with Chapter 47 of the Title 10, United States Code and the Manual for Courts-Martial.

(2) Uses predefined agreements and tactics, techniques, and procedures with the ISSO or ISSM to notify the DoW LE/CI agencies for any LE/CI support requested.

(3) Initiates and supports coordination planning between users, security personnel, LE/CI, vendors, internet service providers, cloud service providers, other CSSPs and other internal or external security components.

(4) Assists LE officials with information gathering for LE/CI investigations and cyber incidents by collecting and retaining specified information on all incidents in support of LE investigations, and/or situational awareness in accordance with established organizational/LE/CI guidance.

(5) Ensures the acquisition and preservation of secure artifacts, evidence, and 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 are in accordance with established organizational and LE/CI chain of custody protocols.

(6) Implements and enforces procedures to prevent unauthorized disclosure of investigative information.

(7) Retains and secures all incident reports and collected information for 1 year.

(8) Provides regular and recurring updates through all phases of the incident handling lifecycle, as identified in policies, procedures, orders, or collaboration requirements.

(9) Conducts incident close out activities as authorized or directed once external partner and supported agencies have completed coordinated response actions.

(10) Conducts post incident after action review with the AO, the ISSM, and the LE officials, at a minimum to identify lessons learned.

c. The ISSM or ISSO:

(1) Complies with appropriate policy guidance for LE/CI and criminal investigations that relate to cyberspace.

(2) Notifies DoW LE/CI agencies responsible for the affected portion of the DoDIN of cyber mission forces deployment, and any LE/CI support requested. If the CSSP did not initiate the investigation into an activity that triggers an insider threat threshold, the DoW entity will work in accordance with the DoDI 5205.16 to coordinate with LE/CI on investigations not initiated by the CSSP that trigger an insider threat threshold.

(3) Cooperates with the CSSP and LE/CI officials supporting information gathering for incidents.

(4) Coordinates with the CSSP to:

(a) 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.

(b) Conduct incident close out activities with the CSSP as authorized or directed once coordinated response actions have been completed, to include post-incident after action review with LE/CI officials, at a minimum to identify lessons learned.

7. Incident Response Analysis.

a. The CSSP:

(1) Performs incident response analysis in accordance with CJCSM 6510.01B. This can consist of volatile data analysis, forensic media analysis, reverse engineering or malware analysis, and intrusion assessments. There is a shared responsibility to provide information between the subscriber and CSSP. The subscriber must make the data available to the CSSP consistent with the incident event category, nature, and severity of impact.

(2) Provides the capability to analyze and respond to events or cyber incidents to mitigate any adverse operational or technical impact on the DoW-owned or -operated portion of the DoDIN in accordance with DoD Directive 5106.01, DoDI 8582.01, and Committee on National Security Systems Instruction (CNSSI) 1010.

(3) Assists to determine the current adequacy of cybersecurity measures, identifies deficiencies, provides data from which to predict the effectiveness of proposed cybersecurity measures, and confirms the adequacy of such measures after implementation.

(4) Reports all findings to the AO, the ISSM, and the ISSO associated with the system or network where the incident was discovered. Additionally, the CSSP reports all findings into the DoW joint incident management system, in accordance with CJCSM 6510.01.

(5) Records any lessons learned in the Joint Lessons Learned Information Systems located at https://jtp.jten.mil/jtp/.

b. The ISSO or ISSM:

(1) Delivers required incident response artifacts to the CSSP.

(2) Specifies the CSSP as the cybersecurity point of contact in all documentation and coordination to allow simultaneous sharing of cyber information.

(3) Ensures the cyber protection team, if assigned, reports to the CSSP to coordinate all incident response activities.

(4) Verifies, validates, and articulates the operational impact of incidents and reports to the CSSP.

(5) Implements passive countermeasures where feasible and notifies the CSSP.

(6) Retains all incident artifacts and documentation in accordance with the approved records disposition schedule for the applicable DoW Components pursuant to DoDI 8530.03. Data collected will be shared with the CSSP, upon request, in accordance with Subpart 204.73 of the Defense Federal Acquisition Regulation Supplement.

c. The cybersecurity activities that a certified CSSP must perform can be found in the CSSP Minimum Cybersecurity Activities Checklist located at: https://cybersecurityks.osd.mil/kscollaboration/CSSP/Pages/CSSPCSActivities.aspx.

8. SUSTAINMENT OF CSSP PERFORMANCE AND CONTINUOUS SELF-ASSESSMENT.

The CSSP:

a. Conducts annual self-assessments of their compliance with DoDI 8530.01.

b. Utilizes DoW cyber assessment teams or automated capabilities approved by USCYBERCOM, based on subscriber needs to determine the best DoW cyber assessment team to obtain the desired result suited for that network/system based on threat.

c. Maintains documentation of all sustainment and self-assessment activities, including test results, corrective actions, and verification artifacts, for review during formal certification evaluation.

d. Ensures sustainment and self-assessment activities are aligned with broader DoW continuous monitoring and risk management frameworks.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ACRONYM	MEANING
AO	authorizing official
ATO	authorization to operate
BCAP	boundary cloud access point
CDRUSCYBERCOM	Commander, United States Cyber Command
CI	counterintelligence
CJCSM	Chairman Joint Chiefs of Staff manual
CNSSI	Committee on National Security Systems instruction
CPCON	cyber protection condition
CSSP	cybersecurity service provider
DCDC	Department of Defense Cyber Defense Command
DCSA	Defense Counterintelligence and Security Agency
DoDI	DoD instruction
DoDIN	Department of Defense information network
DoDM	DoD manual
DoW	Department of War
DoW CIO	DoW Chief Information Officer
DTM	directive-type memorandum
GENSER	general service
IAP	internet access point
IC	Intelligence Community
ICD	Intelligence Community directive
ISSM	information system security manager
ISSO	information system security officer
LE	law enforcement
OSW	Office of the Secretary of War
SAP	special access program
SCI	sensitive compartmented information
TS	TOP SECRET
USCYBERCOM	United States Cyber Command

PART II. DEFINITIONS

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

TERM	DEFINITION
attribution	The correlation between an internet protocol address; domain; tactic, techniques, and procedures; or other indicators to associate activity to tracked intrusion sets or adversarial activity.
coalition or mission partner environment	Defined as "MPE" in DoDI 8110.01.
continuous	24 hours a day, 7 days a week.
CSSP	Defined as "cybersecurity service provider" in DoDI 8530.01.
CSSP alignment	A CSSP that meets, at a minimum, the standards in Attachment 4 and in the CSSP Minimum Cybersecurity Activities Checklist found at: https://cybersecurityks.osd.mil/kscollaboration/CSSP/Pages/CSSPCS Activities.aspx.
cyber incident	Defined as "incident" in CNSSI 4009.
cyber terrain	Defined as "key terrain in cyberspace" in Joint Publication 6-0.
cybersecurity entity	A DoW Component or subcomponent responsible for performing one or more cybersecurity activities internally or externally on behalf of their Component.
defensive cyber operation – internal defensive measures	Defined in the DoD Dictionary of Military and Associated Terms.
DoDIN	Defined in the DoD Dictionary of Military and Associated Terms.
DoDIN operations	Defined in the DoD Dictionary of Military and Associated Terms.
DoW CSSP subscriber	A designated organization within the DoW that collaborates with a CSSP to manage and protect the DoW information network against cyber threats. This partnership involves the DoW Component heads and other designated organizations that oversee network operations and cybersecurity activities. The DoW CSSP program aims to ensure that authorized service providers effectively protect the DoW portion of the cyberspace domain.

TERM	DEFINITION
DoW entities	DoW organizations that perform cybersecurity activities that are inherently governmental functions that must be performed by, or under the direct oversight and responsibility of, a DoW Component head. The performance of cybersecurity activities includes reporting to and collaboration with the aligned CSSP.
exploit	Defined in International Organization for Standardization International Electrotechnical Commission 27039:215.
information	Defined in CNSSI 4009.
inherently governmental function	Defined in Part 7 of the Federal Acquisition Regulation.
intelligence network	Information system(s) implemented with a collection of interconnected components belonging to one of the 18 U.S. executive branch agencies and organizations that comprise the IC.
intrusion	Defined in CNSSI 4009.
malicious activity	Defined in CNSSI 4009 as “malicious cyber activity”.
network	Defined in CNSSI 4009.
opportunity	Defined in National Institute of Standards and Technology Interagency or Internal Report 8286.
SAP	Defined in CNSSI 4009.
system	Defined in CNSSI 4009.
threat actor	Defined in National Institute of Standards and Technology Special Publication 800-150.
vulnerability	Defined in CNSSI 4009.