DoD Manual 8530.01

Cybersecurity Activities Support Procedures

Originating Component:	Office of the DoD Chief Information Officer
Effective:	May 31, 2023
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Cancels:	DoD O-8530.1-M, "Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Program," December 17, 2003
Approved by:	John Sherman, DoD Chief Information Officer

Purpose: In accordance with the authority in DoD Directive (DoDD) 5144.02 and the policy and guidance in DoD Instruction (DoDI) 8530.01, this issuance assigns responsibilities and provides procedures for designated DoD Component-level organizations directing and managing network operations and cybersecurity activities and supporting cybersecurity service providers (CSSPs) to protect the Department of Defense information network (DODIN) against unauthorized activity, vulnerabilities, or threats.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

This issuance applies to OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

SECTION 2: RESPONSIBILITIES

2.1. DOD CHIEF INFORMATION SECURITY OFFICER (DOD CISO).

Under the authority, direction, and control of the DoD Chief Information Officer, the DoD CISO:

a. Oversees the authorization process for DoD Component-level organizations directing and managing network operations and cybersecurity activities and confirms DoD Component compliance with criteria established in Appendix 4A.

b. Coordinates with the Commander, United States Cyber Command (CDRUSCYBERCOM) to maintain a cybersecurity service assessment program to assess the DoD Components' cybersecurity services.

c. Grants non-DoD Federal mission partners a DoD CSSP equivalency rating based on the results of their CSSP assessment.

d. Oversees development of the DoD Cybersecurity Services Evaluator Scoring Metrics (ESM) for assessment teams to measure cybersecurity service implementation by DoD Component-level organizations directing and managing network operations and cybersecurity activities.

e. Coordinates with the CDRUSCYBERCOM in assessing the effectiveness, efficiency, and performance of the DoD Components directing and managing cybersecurity activities and supporting CSSPs. If necessary, revokes designation of a Component's CSSP.

f. In coordination with the CDRUSCYBERCOM, provides guidance for cloud service providers to share defensive cyberspace operations (DCO) incident reporting and mitigations to resolve DCO incidents and findings with DoD CSSPs.

g. Establishes an assessment and designation process for commercial entities performing CSSP activities, including information sharing of the results from external assessments.

h. Resolves disagreements involving the cybersecurity assessment team and a DoD Component.

i. Establishes an assessment and designation process for commercial entities performing CSSP activities.

2.2. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE.

Under the authority, direction, and control of the Under Secretary of Defense for Intelligence and Security; the authority, direction, and control exercised by the DoD Chief Information Officer over the activities of the Cybersecurity Directorate, or any successor organization, of the

National Security Agency, funded through the Information System Security Program; and in addition to the responsibilities in Paragraph 2.3, the Director, National Security Agency/Chief, Central Security Service, in coordination with the DoD CISO:

a. Provides cybersecurity best practices used to assess the effectiveness and performance of DoD Component-level organizations directing and managing network operations and cybersecurity activities and supporting CSSPs.

b. Provides technical solutions that enhance cybersecurity protection, detection, and response.

c. Provides analyses of warning intelligence, threats, suspicious or malicious network traffic, and attacks.

(1) Conducts attack sensing and warning (AS&W) to identify the potential impact to operations or missions (e.g., increased intrusion detection system (IDS) alerts, logs, loss of service, file transfer protocol port blocked) through analysis of available alert and traffic flow systems.

(2) Develops countermeasures based on analysis of AS&W information.

(3) Correlates warning intelligence, AS&W information, cyber events, and sensor data to search for advanced, persistent, and coordinated threats across multiple networks.

(4) Develops countermeasures to address threats to operations identified by analysis of warning intelligence information.

d. Provides technical and analytical support to DoD Components as requested by the CDRUSCYBERCOM.

2.3. DOD COMPONENT HEADS.

The DoD Component heads:

a. Require that cybersecurity activities are performed for all DoD Component systems and technology in accordance with DoDI 8530.01.

b. Designate a DoD Component-level organization to coordinate, direct, and manage network operations and cybersecurity activities.

c. Support and implement DoD-wide cybersecurity operational direction from the CDRUSCYBERCOM.

d. Provide access to DoD Component capabilities, assets, and data to DoD inspection, assessment, and red team(s). If using commercial services, the DoD Component is responsible for coordinating access for DoD assessment and red team(s).

e. As a condition to grant an authorization to operate, require alignment to a DoD Component-level organization directing and managing network operations and cybersecurity activities or authorized CSSPs for cybersecurity services.

f. Require that management of networks and cybersecurity operations are fully coordinated and integrated with the cybersecurity evaluation process.

g. Maintain an inventory of information technology (IT) systems and networks authorized in accordance with DoDI 8510.01 and identify their DoD Component-level organization directing and managing network operations and cybersecurity activities and supporting CSSPs. The DoD Component's IT service provider maintains the supporting authorized IT systems and networks inventory.

h. Verify that connections registered in the Defense Information Systems Agency Network Approval Process Database or Secure Internet Protocol Router Network Global Information Grid Interconnection Approval Process System Database are aligned with a DoD Component-level organization directing and managing network operations and cybersecurity activities and supporting CSSP.

i. Coordinate with cloud service providers to share DCO incident reporting and mitigations to resolve DCO incidents and findings with DoD CSSPs.

j. Require the organic entities and contracted CSSPs providing cybersecurity services be authorized in accordance with established DoD requirements and Appendix 4A.

k. Establish and maintain records identifying the authorized external service providers and the cybersecurity activities provided to their organization.

2.4. CDRUSCYBERCOM.

In addition to the responsibilities in Paragraph 2.3., the CDRUSCYBERCOM:

a. Coordinates global DODIN operations and DCO-internal defensive measures (DCO-IDM) to support operational requirements that fall outside of the DoD Component's authority, capabilities, and capacity.

b. In accordance with DoDI 8530.01, performs evaluations to assess the effectiveness and performance of primary DoD Component-level organizations directing and managing network operations and cybersecurity activities and supporting CSSPs with support, as needed, from the Defense Intelligence Agency (DIA) and Special Access Program Central Office for:

(1) Unclassified and classified collateral information systems (ISs).

(2) The Joint Worldwide Intelligence Communications System (JWICS), with evaluations scheduled, coordinated, and conducted by the DIA, and with releasable data selected and organized by the DIA and shared with the CDRUSCYBERCOM.

(3) Systems that support special category information (e.g., special access program, sensitive compartmented information, or other compartmented information).

c. Develops and revises DoD Cybersecurity Services ESM as the criterion for cybersecurity authorization assessments based on the cybersecurity activities mapped to the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity in DoDI 8530.01 and this issuance.

d. Develops a formal DoD cybersecurity service assessment program that includes:

(1) Mission-based cyber threat inspections to validate the DoD Component's ability to conduct its mission and protect its assets and capabilities in accordance with DoD requirements and directives from United States Cyber Command (USCYBERCOM).

(2) Verification and assessment of DoD Component-wide coverage for all required cybersecurity activities and recommendations for remediation of cited shortfalls.

(3) A cybersecurity service validation process for the execution and delivery of cybersecurity services to a DoD Component by another DoD Component's authorized CSSP are conducted in accordance with DoDI 8530.01.

(4) Confirmation that any services a DoD Component performs outside of any agreement with an authorized CSSP are evaluated in accordance with the objectives of the cybersecurity service evaluation process.

e. Provides experienced technical members to conduct CSSP assessments.

f. Provides approval for DoD Components and CSSP support internally to the DoD Component or externally to other DoD Components.

g. Monitors changes in DoD Component and CSSP certification status, tracks CSSP plan of action and milestones (POA&M), and conducts cybersecurity authorization assessments every 3 years, or when the CSSP's authority to operate (ATO) expires.

h. Oversees the implementation and execution of the CSSP approval process in coordination with the DoD CISO and DIA.

i. Coordinates relevant cybersecurity issues and requirements between the DoD Component-level organizations directing and managing network operations and cybersecurity activities and supporting CSSPs.

j. Develops, maintains, and updates a cybersecurity evaluation education, training, and awareness program.

k. Provides cybersecurity technical, analytical, and coordination support to Service Cyber Components, DoD Components, Federal mission partners, and supporting CSSPs conducting missions on the DODIN.

l. Coordinates with the DoD CISO to develop a cybersecurity service assessment program to assess the DoD Component's cybersecurity services, review Components' performance, and, if necessary, revoke designation of a Component's CSSP.

SECTION 3: DOD COMPONENT ACTIVITIES TO PROTECT THE DODIN

3.1. GENERAL.

a. This section identifies a set of cybersecurity activities that are required for DODIN operations and DCO-IDM to protect the DODIN.

b. These activities include, but are not limited to:

(1) Vulnerability assessment and analysis.

(2) Vulnerability management.

(3) Malware protection.

(4) Information security continuous monitoring (ISCM).

(5) Cyber incident handling.

(6) DODIN user activity monitoring for the DoD Insider Threat Program.

(7) Warning intelligence and AS&W.

c. The functional requirements of cybersecurity activities as described in DoDI 8530.01 reside with the DoD Component heads.

(1) DoD Component heads must designate a DoD Component-level organization to direct and manage network operations and cybersecurity activities for the Component. The DoD Component is responsible for ensuring that all the cybersecurity activities listed in Paragraphs 3.2. through 3.8. are performed.

(2) Cybersecurity services may be obtained from within a DoD Component or from an authorized external CSSP. All DoD entities that are providers must be authorized in accordance with the cybersecurity assessment program. The DoD Component head is responsible for all risk management decisions and for oversight of the cybersecurity capabilities and services provided to them by a commercial entity to ensure that they are in accordance with the cybersecurity assessment program.

(3) The DoD Component head will verify that cybersecurity activities and acquired services meet established evaluation criteria and performance measures whether these services are performed organically, by an authorized DoD CSSP, or by a commercial entity. The DoD Component will maintain an information security program plan.

(4) The DoD Component head will provide cybersecurity training.

(5) The DoD Component head will develop and maintain information security architectures for systems, assets, and capabilities where they are designated as the authorizing

official (AO). The information will include, at a minimum, Internet protocol location, medium access control, and other information to facilitate DCO-IDM efforts.

d. The DoD will retain cybersecurity activities that directly support decisions regarding the acceptance of risk in accordance with DoD Cybersecurity Activities Performed for Cloud Service Offerings and active DCO-IDM supported by potentially classified intelligence community information. The cybersecurity activities performed by a DoD entity are described in Paragraphs 3.2. through 3.8.

e. Commercial entities can perform cybersecurity activities that are not specifically identified as activities for DoD entities.

(1) The commercial entity will comply with DoD Component information security requirements in accordance with DoDI 8582.01.

(2) A formal agreement must detail the arrangement and expectations between the DoD Component and the commercial entity for establishing, measuring, testing, and maintaining a required level of performance.

(3) The commercial entity will comply with personnel security requirements in accordance with DoDI 5200.02.

3.2. VULNERABILITY ASSESSMENT AND ANALYSIS ACTIVITIES.

a. The DoD Component will perform a risk assessment of assets and capabilities when they are designated as the AO in accordance with DoDI 8510.01. The DoD Component will maintain an assessment plan. The DoD Component AO will select the vulnerability assessments that best fit the need of the application or mission system. The DoD Component AO has the option to choose one or more of the vulnerability assessments in Paragraphs 3.2.a.(1)–(4), but only one is required annually.

(1) The DoD Component will conduct intrusion assessments to identify if data has been compromised, highlight unauthorized activity, identify any critical vulnerabilities, and provide direction for the enhancement of local mission owner cyber defense. The DoD Component will:

(a) Maintain the results and remediation recommendations from the intrusion assessments in accordance with Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01F.

(b) Maintain status of vulnerability remediation in the POA&M for the asset or capability.

(2) Authorized individuals conducting penetration testing assessments in accordance with DoDI 8531.01 without the common knowledge by the assessed organization except for a trusted agent network and approval by the DoD Component. The DoD Component will:

(a) Identify the exploited vulnerable points of the in-scope targets and determine general remediation recommendations.

(b) Track and execute corrective actions and mitigations for identified vulnerabilities.

(c) Conduct DoD Cyber Red Team operations in accordance with CJCSI 6510.05. This cybersecurity activity must be performed by an accredited DoD Cyber Red Team.

(3) The DoD Component will conduct cyberspace operational assessments (e.g., operational exercises with a cyber-component).

(4) The DoD Component will conduct cyber security inspections (e.g., Component inspector general, command cyber readiness inspections).

b. The DoD Component will:

(1) Perform network and host vulnerability scanning in accordance with CJCSI 6510.01F and DoDI 8531.01.

(2) Conduct vulnerability scans in accordance with USCYBERCOM guidance (e.g., frequency, method, capability).

(3) Identify open and unauthorized transmission control protocol/user datagram protocol ports in accordance with DoDI 8551.01.

(4) Identify misconfigurations and vulnerabilities in operating systems, applications, services, and any other software.

(5) Take appropriate actions to correct findings in a prioritized manner and validate the effectiveness of executed actions. Priority should be given to exploitable vulnerabilities that could negatively impact mission success, should they be successfully exploited.

(6) Maintain status of vulnerability remediation in a POA&M for the asset or capability.

c. The DoD Component will provide the CDRUSCYBERCOM visibility and insight into the cybersecurity status of the DoD Components' respective assets and capabilities when they are designated as the AO to assess risk to the DODIN through reports, findings, and analyses resulting from vulnerability assessments, intrusion assessments, evaluations, inspections, exercises, DoD Cyber Red Team operations, or lessons learned from military operations. A DoD entity must perform the actions in Paragraphs 3.2.c.(1)–(3):

(1) Analyze vulnerability assessments and report results in accordance with DoDI 8531.01.

(2) Analyze network and host vulnerability scan results and provide copies of results and recommendations to USCYBERCOM.

(3) Establish a formal vulnerability assessment and analysis improvement process by capturing lessons learned from the analysis of mitigation actions from vulnerability and intrusion assessments, exercises, and DoD Cyber Red Team operations.

3.3. VULNERABILITY MANAGEMENT.

The DoD Component will:

a. Require an enterprise management, technology-driven system inventory including hardware equipment, operating systems, software applications, and user authorities that apply DoD-required and organization-accepted standard security configurations in accordance with DoDI 8531.01.

b. Provide the capability to receive open-source, official, and classified threat, vulnerability, and attack notifications and take directed corrective actions to mitigate potential vulnerabilities or threats to the DoD Component's assets and capabilities where they are designated as the AO in accordance with DoDI 8531.01 and as described in NIST Special Publication (SP) 800-40.

c. Establish a vulnerability management process and procedures in accordance with DoDI 8531.01 that provide positive control to implement actions on the DoD Component-owned or -operated assets and capabilities where they are designated as the AO in accordance with CDRUSCYBERCOM orders or other directives such as tasking orders, vulnerability management alerts, directives for patching, or directives for configuration changes. This cybersecurity activity must be performed by a DoD entity.

d. Verify that DoD Component organizations implement capabilities to expose management repository information to support higher-level reporting and vulnerability trend analysis in accordance with DoDI 8531.01.

3.4. MALWARE PROTECTION PROCESS.

The DoD Component will:

a. Provide the capability to prevent, detect, contain, and eradicate malware as described in NIST SP 800-83.

(1) Employ malware protection capabilities on applicable DoD IS to protect against known malware variants.

(2) Verify that signature-based malware protection capabilities are kept up to date with the latest malware signatures and maintain an exception list for deployed signatures.

(3) Verify that heuristic-based malware protection capabilities are properly configured and tuned to protect against malware variants that are difficult to detect and prevent via signature-based capabilities.

(4) Where possible, leverage technologies such as containment and virtualization to prevent, minimize the damage of, and contain the spread of malware.

b. Configure malware detection mechanisms to perform periodic scans within the DoD IS where they are designated as the AO of the DODIN in accordance with current DoD and DoD Component guidance.

(1) Implement the capability to detect and prevent malware incidents (e.g., malicious code, malicious logic, malicious applets) by employing malware detection and remediation mechanisms to detect and remove malware.

(2) Configure network monitoring detection capabilities with automatic alerts from mail or other servers showing actions for potential malicious payloads.

(3) Implement spam protection measures.

(4) Configure malware detection capabilities to actively detect malware by ensuring that anti-malware software, engines, and signatures are current.

(5) Coordinate malware scan events to minimize operational or mission impact.

(6) Prioritize IS malware detection responses based on mission impact.

(7) Implement automated pre-approved actions in response to malware detection.

c. Alert application and system owners of new malware. This cybersecurity activity must be performed by a DoD entity.

3.5. ISCM.

a. To maintain ongoing awareness of information security status, threats, and vulnerabilities as described in NIST SP 800-137A to support organizational risk management decisions, the DoD Component will:

(1) Perform continuous monitoring of assets and asset information (e.g., Internet protocol address, domain, system criticality, configuration compliance, vulnerability, exposure) to include, at a minimum, Internet protocol location and medium access control to facilitate DCO-IDM efforts.

(2) Maintain 24-hour access to sensor data from deployed network-based sensors for all security domains monitored.

(3) Maintain access to current (no more than 365 days old) network architecture diagrams showing placement of sensors (e.g., IDS, intrusion prevention systems, routers, netflow/packet capture systems, firewalls).

(4) Maintain awareness and understand how to support mission requirements through cyber event analysis, mission briefs, risk mitigation, and key terrain identification.

b. The DoD Component will support DODIN operations by providing ongoing awareness of threats and security status of traffic, fault, performance, bandwidth, route, and associated network management areas. ISCM also supports the monitoring of employee use of the DODIN to detect anomalous activity in accordance with DoDD 5205.16.

(1) Perform correlation of asset information with supporting threat and vulnerability data to maintain awareness of overall security posture. This cybersecurity activity must be performed by a DoD entity.

(2) Incorporate results from continuous monitoring activities into risk management decisions. This cybersecurity activity must be performed by a DoD entity.

(3) Collect and analyze network traffic, fault, performance, and bandwidth information; alerts; and data to augment detection of network anomalies and potential unauthorized activity.

c. The DoD Component will support DODIN operations and DCO-IDM by providing ongoing awareness of cyber events and incidents. This capability supports timely, informed, and actionable cyber incident handling decisions in accordance with Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B. This cybersecurity activity and those described in Paragraphs 3.5.c.(1) and 3.5.c.(2) must be performed by a DoD entity.

(1) Establish processes to support identification of reportable cyber events and incidents through continuous monitoring and analysis of cyber activity coupled with threat intelligence correlation.

(2) Provide ongoing awareness of reportable cyber events and incidents through continuous event management updates, consistent shift turnover of events and incidents, recurring incident awareness briefs, updating event and incident analysis records, and maintaining event/incident dashboards.

d. The DoD Component will support the risk management framework by providing ongoing awareness and security status of the posture of an organization's information and systems. This capability supports timely, informed, and actionable risk decisions and continued risk management framework decisions in accordance with DoDI 8510.01.

(1) Conduct security control assessments through the review of current security authorization packages (e.g., security plans, security assessment reports, and POA&M).

(2) Coordinate changes to security authorizations with system owners and the AO as required.

3.6. CYBER INCIDENT HANDLING PROGRAM.

The DoD Component will:

a. Perform cyber incident handling in accordance with CJCSM 6510.01B and Committee on National Security Systems Instruction (CNSSI) No. 1010 and as described in NIST SP 800-61. Provide training to incident response personnel.

(1) Determine event and incident categories in accordance with CJCSM 6510.01B and characterize event/incidents (e.g., insider threat activity, advanced persistent threat). This cybersecurity activity must be performed by a DoD entity.

(2) Maintain initial triage and incident response processes for cyber events/incidents, which include event/incident prioritization and course-of-action development.

(3) Provide the CDRUSCYBERCOM with visibility and insight into detected cyber incidents. This cybersecurity activity must be performed by a DoD entity.

(4) Report and update events and incidents within timelines established in CJCSM 6510.01B. Include a description of attack methods and potential operational or mission impact. This cybersecurity activity must be performed by a DoD entity.

(5) Develop and deploy tailored countermeasures. Eradicate malware and prevent spread or reinfection.

b. Conduct the acquisition and preservation of data associated with cyber intrusion incidents, investigations, and operations in accordance with NIST SP 800-61.

(1) Provide forensically sound acquisition and preservation of incident data, which includes volatile (e.g., system registers, cache, random access memory), persistent (e.g., system images, system logs, malware, network logs, and network flow), and configuration data, as applicable.

(2) Implement a process to collect relevant incident data (e.g., shutdown/disconnect policy, related system data collection) with incident reports and data retained for 1 year and source and method information data retained for 5 years.

(3) Verify that cybersecurity logs management considers volume, variety, veracity, and velocity of data requirements.

c. Report all incidents that appear to be violations of Federal law to DoD Component criminal investigative organizations, law enforcement organizations, the Defense Criminal Investigative Service, or the Office of Inspector General of the Department of Defense. A DoD entity must perform the actions in Paragraphs 3.6.c.(1)–(4):

(1) Report incidents involving loss of sensitive or classified information to law enforcement or counterintelligence, as required.

(2) Report incidents involving cleared defense contractor sites to the Defense Counterintelligence and Security Agency, as appropriate.

(3) Report incidents involving personally identifiable information to the DoD Component and the Senior Agency Official for Privacy as applicable, in accordance with DoDI 5400.11, Volume 2 of DoD Manual 5400.11, and DoD Manual 6025.18 for incidents involving protected health information.

(4) Incidents involving unclassified networks of defense contractors will be reported to the DoD Defense Industrial Base Collaborative Information Sharing Environment at https://dibnet.dod.mil/ in accordance with Defense Federal Acquisition Regulation Supplement 252.204-7012.

d. Safeguard classified and controlled unclassified information against unauthorized disclosure in accordance with Volume 3 of DoD Manual 5200.01, DoDIs 5200.48 and 5400.11, Volume 2 of DoD Manual 5400.11, DoD 5400.11-R, DoD Manual 6025.18, CJCSM 6510.01B, Committee on National Security Systems Policy No. 18, and CNSSI No. 1001.

(1) Implement containment measures to regain control of or to isolate affected systems to prevent further malicious activity.

(2) Contain the spread of malware to prevent further damage to IT systems through initial malware detection, analysis and identification, and execution of containment measures.

e. Implement cyber incident mitigation efforts by identifying root causes and coordinating implementation of recovery operations. Restore system functionality by rebuilding systems in accordance with accredited baselines and current security guidelines, directives, and orders.

3.7. DODIN USER ACTIVITY MONITORING FOR A DOD INSIDER THREAT PROGRAM.

The DoD Component will implement cybersecurity monitoring activities as part of a DoD Component insider threat program established in accordance with DoDD 5205.16 and Intelligence Community Standard 500-27 or as otherwise directed by the Office of the Director of National Intelligence. This includes tools to monitor employee use of IT systems, personnel assigned to monitor and detect anomalous activity by employees, separation of duties for accountability, evaluation of detected events to identify insider threat activity, and ensuring that incident handling processes are followed for insider threat activities. A DoD entity must perform the actions in Paragraphs 3.7.a.–c.:

a. Implement the minimum capabilities to monitor user activity and audit information by unclassified and classified collateral and JWICS users.

(1) Develop an insider threat advanced detection capability with defined triggers. This capability must have the ability to alert, or display in near real-time, events that are indicative of potential insider threat activity.

(2) Integrate a monitoring capability to collect user activity data, including key stroke monitoring, full application content, screen capture, and file shadowing.

(3) Direct user activity data to subscribers while protecting data at rest, in use, and in transit in accordance with applicable law, policy, and regulations regarding civil liberties and privacy protections.

b. Assign personnel to monitor and detect anomalous user activity and establish separation of duties for accountability.

(1) Establish insider threat duties based on the subscriber's perceived threat levels and prioritizations and available resources.

(2) Develop an oversight process to review the activities of personnel with privileged access to sensitive information to verify that duties are being performed ethically and in accordance with legal, civil liberties, and privacy protections.

c. Establish proper incident handling and reporting procedures in accordance with CJCSM 6510.01B, DoDI 5400.11, and Volume 2 of DoD Manual 5400.11.

(1) Report insider threat activity to the appropriate DoD Component insider threat hubs using the Joint Incident Management System. For non-24-hour operational hub environments, service providers must have an alternative point of contact to report insider threat activity within the appropriate reporting timelines.

(2) Preserve data integrity for evidentiary purposes and follow applicable chain-of-custody guidelines for transferring information.

(3) Adhere to the USCYBERCOM reporting timelines specific to the categories of reportable cyber incidents and events and impact severity levels.

3.8. WARNING INTELLIGENCE AND AS&W.

a. The DoD Component will provide the capability to receive notice of warning intelligence information provided by intelligence organizations such as the DIA and the National Security Agency. A DoD entity must perform the actions in Paragraphs 3.8.a.(1)–(2):

(1) Receive and perform preliminary analysis on warning intelligence from approved sources.

(2) Share warning intelligence notifications, notes, reports, and information with USCYBERCOM and DoD Components.

b. The DoD Component will support analysis of threats, suspicious or malicious network traffic, and attacks.

(1) Conduct AS&W to identify potential impact to operations or missions (e.g., increased IDS alerts, logs, loss of service, file transfer protocol port blocked) through analysis of available alert and traffic flow systems.

(2) Develop countermeasures based on analysis of AS&W information.

(3) Correlate warning intelligence, AS&W information, cyber events, and sensor data to search for advanced, persistent, and coordinated threats across multiple networks. This cybersecurity activity must be performed by a DoD entity.

(4) Develop countermeasures to address threats to operations identified by analysis of warning intelligence information. This cybersecurity activity must be performed by a DoD entity.

(5) Exchange intelligence notifications, AS&W information, threat analysis, or warnings and potential courses of action (e.g., countermeasure and/or mitigation recommendations) with USCYBERCOM and DoD Components (e.g., tippers, situational awareness reports). This cybersecurity activity must be performed by a DoD entity.

c. The DoD Component will enable the prevention or mitigation of impact to the DoD Component-owned or -operated assets and capabilities where they are designated as the AO.

(1) Develop and implement tailored countermeasures to prevent or mitigate potential cyber event impacts to the DODIN.

(2) Share countermeasures with USCYBERCOM. This cybersecurity activity must be performed by a DoD entity.

3.9. ACCOUNTABILITY.

The CDRUSCYBERCOM holds organizations accountable for implementing the DoD Component activities outlined in this section, including actions directed by DoD Component heads to protect the DODIN.

a. Comply with DoD, intelligence community, and DoD Component physical protective measures to secure Component cybersecurity systems.

b. DoD Component internal or external CSSP, who are responsible for implementing cybersecurity services in accordance with DoD Component policy, memorandums of agreement (MOAs), or contracts, will:

(1) Maintain a quality assurance program.

(2) Use quantitative analysis to measure performance of cybersecurity activities.

(3) Establish DoD Component frequency for measuring the operational effectiveness of cybersecurity activities with measurements such as simulated unauthorized network activity

(e.g., port scanning, phishing); cybersecurity event/incident drills (e.g., procedure-based tabletop exercises, event walk-throughs); or vulnerability management results (e.g., vulnerability compliance statistics, support responsiveness).

SECTION 4: CYBERSECURITY INTEGRATION INTO DODIN OPERATIONS

4.1. CYBERSECURITY ACTIVITIES INTEGRATION.

a. DoD Components will organize and integrate cybersecurity activities to support DODIN operations and DCO-IDM in accordance with published orders and directives.

b. DoD Component subordinate organizations and AOs responsible for ISs will comply with orders or directives from the CDRUSCYBERCOM and their DoD Component authority designated to direct the security, operations, and defense of the DoD Component's assets and capabilities.

c. DoD Components will exercise operational control over their supporting CSSPs pursuant to support agreements, MOAs, and contracts or in accordance with DoD Component guidance.

d. DoD Components will require that contracted services allow for the movement and maneuvering of DoD cyberspace defensive forces for incident response.

4.2. CSSP.

a. DoD Components must designate a Component-level organization to direct and manage network operations and cybersecurity activities mapped to the NIST Framework for Improving Critical Infrastructure Cybersecurity as the focal point for implementing and conducting Component-wide cybersecurity activities for DODIN operations and DCO-IDM. Where cybersecurity services for a Component are distributed among multiple authorized external providers, supporting providers will assist the designated Component-level organization in the coordination and integration of Component cybersecurity through information sharing in accordance with DoDI 8320.02 and DoDD 8000.01.

b. In accordance with DoDI 8530.01, a CSSP will:

(1) Have the capability to provide cybersecurity services for some or all cybersecurity activities.

(2) Execute cybersecurity responsibilities and authorities in accordance with DoD Component policy, MOAs, contracts, or support agreements.

(3) Comply with directives and orders of the CDRUSCYBERCOM and supported DoD Component-level organizations directing and managing network operations and cybersecurity activities.

(4) Document all supported entities and associated systems in accordance with DoD Component policy, MOAs, and contracts or support agreements.

APPENDIX 4A: DOD COMPONENT CYBERSECURITY ASSESSMENT

4A.1. AUTHORIZATION PROCESS.

The cybersecurity service evaluation process is based on a four-phase approach ultimately leading to the approval of cybersecurity services for DoD Component organizations and external CSSPs. The cybersecurity service evaluation process provides the DoD with a standardized means to assess a DoD Component-level organization directing and managing network operations and cybersecurity activities and supporting CSSPs based on identified performance criteria (DCO-IDM best practices, self-assessment tools, and DoD requirements) in the DoD Cybersecurity Services ESM. The phases include initiation, evaluation, reporting, and maintenance.

a. Phase 1: Initiation.

(1) Purpose.

The initiation phase begins the 3-year cycle for the cybersecurity service evaluation process.

(2) Activities.

Phase 1 consists of four activities: evaluation notification, evaluation package submission, evaluation package review, and evaluation package acceptance. These activities compile the information necessary for identifying cybersecurity service alignment, supporting documentation for cybersecurity services performed, and a DoD Cybersecurity Services ESM self-assessment.

(3) Evaluation Notification.

The CDRUSCYBERCOM is responsible for maintaining the schedule for upcoming cybersecurity service evaluations. The schedules will be updated regularly and made available to the cybersecurity community. The evaluator is responsible for notifying each entity that will be assessed 120 days in advance of its scheduled evaluation. The evaluation notification will include all requirements and directions for submission of an evaluation package.

(4) Evaluation Package Submission.

Before its scheduled evaluation, each entity to be assessed is responsible for submitting and updating a formal evaluation package to the evaluator for review. The evaluation package contains all documentation applicable to cybersecurity service operations and this process. For classified documentation, the assessed entity will submit a point of contact with a phone number and an e-mail address that will provide the information via secure channels, when requested.

(5) Evaluation Package Review.

Personnel are assigned to review, analyze, and discuss all furnished documentation. The number of evaluators assigned will vary depending on the organization size, scope of services being evaluated, and classification of the data handled. If an evaluation package contains insufficient documentation, the lead evaluator will coordinate with the assessed entity to resolve any discrepancies.

(6) Evaluation Package Acceptance.

Phase 1 concludes with the acceptance of the evaluation package. If the package is accepted, it will continue the evaluation process and the CDRUSCYBERCOM will coordinate with the entity to schedule an on-site evaluation.

(a) The CDRUSCYBERCOM may require the entity to implement corrective actions regarding the self-assessment results and specific performance metrics before the on-site evaluation.

(b) The CDRUSCYBERCOM may determine that the entity does not have sufficient supporting documentation to be able to obtain approval to provide services. When this occurs, the entity will provide justification to the DoD CISO. The DoD CISO will determine the final disposition of the evaluation package.

b. Phase 2: Evaluation.

(1) Purpose.

The evaluation team assesses the target entity along with any cybersecurity organizations under the direction of that entity.

(2) Activities.

The evaluation determines whether the assessed entities' DCO-IDM effectiveness meets the standard established in the DoD Cybersecurity Services ESM. Evaluation activities verify measures of performance and measures of effectiveness within the scope of the assessed entities' mission. Evaluation activities are dependent on the types of enclaves (unclassified and classified collateral ISs, JWICS, and systems that support special category information (e.g., special access programs, sensitive compartmented information, or other compartmented information)) under the assessed entities' purview.

(3) Evaluation Methodology.

The evaluation teams will use the DoD Cybersecurity Services ESM for assessing the DoD Component-level organization directing and managing network operations and cybersecurity activities and supporting CSSPs.

(4) Evaluation Process.

The team will accomplish the activities described in Paragraphs 4A.1.b.(4)(a)–(b) during the evaluation:

(a) A CSSP assessment brief.

(b) Service evaluation.

1. Review the evaluation package provided.

2. Evaluate the effectiveness of the DCO-IDM defense-in-depth methodology performed by the mission owner, CSSPs, and program managers.

3. Observe demonstrations of cybersecurity DODIN defense-in-depth attained by the assessed entity and DODIN boundary defense hierarchy above the assessed entity.

4. Inject cyber effects through Red Team effects in order to measure the effectiveness of cybersecurity service implementation.

5. Document, observe, and recommend DCO-IDM effectiveness and best practices conducted on the DODIN.

6. Provide an out-brief to assessed entities personnel and leadership.

c. Phase 3: Reporting.

(1) Purpose.

In the reporting phase, the evaluation team prepares and delivers an authorization recommendation along with an assessment out-brief to the appropriate DoD Component AO. The assessed entity must provide a POA&M, including a corrective action plan, no later than 30 days after the out-brief. The CDRUSCYBERCOM will review and make an authorization decision based on the findings and recommendations. The reporting phase concludes with an authorization decision sent to the assessed entity, their evaluator, and the DoD CISO for tracking and situational awareness.

(2) Activities.

(a) Reporting.

The evaluation team prepares an authorization recommendation for the assessed entity along with the assessment out-brief and first POA&M submission that the assessed entity provides, if required. The authorization recommendation is submitted to the CDRUSCYBERCOM 45 days after the out-brief. The authorization recommendation letter provides an overall assessment of cybersecurity service capability and includes actions recommended to refine cybersecurity service delivery. The assessment out-brief contains DoD Cybersecurity Services ESM results consisting of observations of processes gathered during the

evaluation and identified deficiencies and recommendations. The evaluation out-brief includes both commendable actions and any weaknesses identified in mission capabilities, practices, and procedures.

(b) Authorization Recommendation.

The evaluator reviews assessment results and POA&M submission, if required, to make an appropriate authorization recommendation to the CDRUSCYBERCOM.

1. If the evaluator determines that the assessed entity complies with the requirements as defined by the DoD Cybersecurity Services ESM, they will issue a letter of recommendation to the CDRUSCYBERCOM. The letter will include a recommendation to authorize all cybersecurity services that met or exceeded the requirement. The evaluator may also make supplemental recommendations to the assessed entity for process improvements.

2. If the evaluator concludes that the assessed entity has not met the requirements defined by the DoD Cybersecurity Services ESM, the authorization letter will include a recommendation to deny authorization or provide an ATO with conditions for any cybersecurity services that did not meet the requirement.

(c) Authorization Decision.

The CDRUSCYBERCOM, in coordination with the DoD CISO, will review the authorization package and make the final decision for the authorization to provide cybersecurity services. Based on the review of the evaluation package from the evaluator, the CDRUSCYBERCOM will grant authorization through an authorization letter or an ATO with conditions. Authorizations are typically granted for a maximum term of 3 years.

(3) ATO with Conditions.

If the CDRUSCYBERCOM elects to award an ATO with conditions, the decision will include the specific reasons for the decision and provide recommendations for the identified deficiencies. An ATO with conditions is granted to any organization that fails to achieve the requirements for each cybersecurity service defined within the DoD Cybersecurity Services ESM.

(a) An ATO with conditions is granted for a minimum of 1 year to a maximum that the CDRUSCYBERCOM determines.

(b) If necessary, as the CDRUSCYBERCOM determines, a re-assessment will be conducted no later than 2 months before the ATO's expiration with conditions.

(c) The CDRUSCYBERCOM may consider or grant an extension to the ATO with conditions.

(4) ATO.

(a) The CDRUSCYBERCOM will award an ATO to the assessed entity achieving the requirements defined in the DoD Cybersecurity Services ESM. The CDRUSCYBERCOM issues the assessed entity a final authorization decision. The decision will contain all recommendations by the evaluators, the DoD CISO, and any supporting documentation.

(b) If the CDRUSCYBERCOM elects to withhold authorization, they issue that decision to the CSSP and include the specific reasons for authorization denial. The evaluation process then reverts to Phase 1.

d. Phase 4: Maintenance.

(1) Purpose.

The maintenance phase includes activities by the authorized entity to maintain its authorized cyber operations and supporting policies and procedures. Entities are required to monitor changes to the cybersecurity mission, perform annual self-assessments, and apply for re-evaluation every 3 years or as needed based on significant changes to the entity's cyber operations as part of this phase.

(2) Activities.

(a) Sustainment.

The authorized entity must maintain its capability for providing effective DCO-IDM and DODIN operations in accordance with requirements defined in the DoD Cybersecurity Services ESM. The authorized entity will accomplish this by sustaining current performance levels and closely monitoring for any changes that may significantly affect mission, personnel, and/or performance. Annually authorized entities will update the CDRUSCYBERCOM with an updated list of subscribers, an alignment matrix, command communications service designators, cloud environment parameters, network architecture, and key standard operating procedures and tactics, techniques, and procedures. If updates are not provided annually, the DoD CISO will be notified.

(b) Self-Assessments.

The authorized entity will perform annual self-assessments using the most current DoD Cybersecurity Services ESM. These evaluations are an effective means of monitoring performance and detecting changes in DCO-IDM and DODIN operations.

4A.2. APPLICATION PROCESS.

The application process consists of the four activities described in Paragraph 4A.2.a.–d.: application package submission, application package review, evaluator's review, and application package acceptance. These activities compile the information necessary for identifying the CSSP organization, services provided, and the subscriber base to be covered. This preliminary

process applies only to organizations that are interested in becoming, or are newly assigned as, a CSSP, not organizations that have already been evaluated and approved as a provider. Those organizations would proceed to Phase 1 of the authorization process to initiate the evaluation process.

a. Application Package Submission.

The prospective CSSP submits a formal application package. The application package contains an application letter, which will serve as an official request to be included in the DoD cybersecurity service evaluation process. In addition, and at a minimum, the prospective CSSP will also submit a package containing:

(1) A CSSP concept of operations.

(2) Cybersecurity services being provided to the DoD Component.

(3) A scope of evaluation environment (e.g., list of command communications service designators, cloud environment parameters).

(4) An alignment matrix including environments being evaluated and the cybersecurity services provided for them.

(5) Network architecture drawings with placement of sensors and other security devices.

(6) A proposed subscriber listing.

(7) A self-assessment using the latest version of the DoD Cybersecurity Services ESM.

b. Application Package Review.

Once the application package is received, it is reviewed by the DoD CISO; then, the appropriate evaluation team is informed. This evaluation team will direct the remainder of the application process.

c. Evaluator's Review.

The CDRUSCYBERCOM will assign appropriate personnel to review, analyze, and assess all furnished documentation. The number of evaluators assigned will vary depending on the prospective organization's size and the scope of services being proposed. Evaluators are selected based on their knowledge, skill, and ability. Evaluators are capable of identifying deviations from applicable governance documentation, performance criteria, and shortfalls in resourcing and providing guidance and recommendations regarding applicant questions or concerns.

(1) Evaluators must be cleared for the classification of the data handled.

(2) If an application package does not contain sufficient documentation, the lead evaluator will coordinate with the mission owner or supporting prospective CSSP to resolve any discrepancies.

(3) The evaluator will collaborate with the mission owner or supporting prospective CSSP to clarify requirements, that the prospective CSSP has properly resourced its cybersecurity effort, and that it is capable of meeting the evaluation criteria.

d. Application Package Acceptance.

The application process concludes with the acceptance of the application package by the CDRUSCYBERCOM and the DoD CISO.

(1) If the mission owner or supporting prospective CSSP's package is accepted, the evaluator will commence the evaluation process. The evaluator will coordinate with the prospective CSSP to begin review of a full evaluation package before scheduling an evaluation, as outlined in Phase 1 of the authorization process.

(2) In some cases, the evaluator may determine during the course of the review of the application package and subsequent discussions that the prospective CSSP is not adequately provisioned and resourced to become a CSSP. When this occurs, the evaluator will provide justification to the CDRUSCYBERCOM. The CDRUSCYBERCOM will then determine appropriate actions based on the circumstances.

4A.3. ASSESSMENT APPEAL PROCESS.

Assessed entities have two opportunities to appeal the results of cybersecurity service assessments:

a. With the evaluator, when initial results are shared with the assessed entity at the conclusion of the assessment.

b. Post assessment with the CDRUSCYBERCOM or their designated representative.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
AO	authorizing official
AS&W	attack sensing and warning
ATO	authority to operate
CDRUSCYBERCOM	Commander, United States Cyber Command
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
CNSSI	Committee on National Security Systems instruction
CSSP	cybersecurity service provider
DCO	defensive cyberspace operations
DCO-IDM	defensive cyberspace operations-internal defensive measures
DIA	Defense Intelligence Agency
DoD CISO	DoD Chief Information Security Officer
DoDD	DoD directive
DoDI	DoD instruction
DODIN	Department of Defense information network
e-mail	electronic mail
ESM	evaluator scoring metrics
IDS	intrusion detection system
IS	information system
ISCM	information security continuous monitoring
IT	information technology
JWICS	Joint Worldwide Intelligence Communications System
MOA	memorandum of agreement
NIST	National Institute of Standards and Technology
POA&M	plan of action and milestones
SP	special publication
USCYBERCOM	United States Cyber Command

G.2. DEFINITIONS.

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

TERM	DEFINITION
AS&W	Defined in CNSSI No. 4009.
collateral information	Defined in CNSSI No. 4009.
continuous monitoring	Defined in CNSSI No. 4009.
CSSP	Defined in DoDI 8530.01.
cybersecurity	Defined in CNSSI No. 4009.
cybersecurity service	Defined in DoDI 8530.01.
cyberspace	Defined in the DoD Dictionary of Military and Associated Terms.
cyberspace operations	Defined in the DoD Dictionary of Military and Associated Terms.
DCO	Defined in the DoD Dictionary of Military and Associated Terms.
DCO-IDM	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.
incident	Defined in CNSSI No. 4009.
incident handling	Defined in CNSSI No. 4009.
insider threat	Defined in CNSSI No. 4009.
intrusion	Defined in CNSSI No. 4009.
IS	Defined in CNSSI No. 4009.
ISCM	Defined in CNSSI No. 4009.
malicious applets	Defined in DoDI 8530.01.
malicious logic	Defined in CNSSI No. 4009.

TERM	DEFINITION
malware	Defined in CNSSI No. 4009.
mission partners	Defined in DoDD 8000.01.
penetration testing	Defined in CNSSI No. 4009.
red team	Defined in CNSSI No. 4009.
risk management framework	Defined in CNSSI No. 4009.
situational awareness	Defined in DoDI 8530.01.
special access program	Defined in CNSSI No. 4009.
unauthorized disclosure	Defined in CNSSI No. 4009.
vulnerability	Defined in CNSSI No. 4009.
vulnerability assessment	Defined in CNSSI No. 4009.
warning intelligence	Defined in the DoD Dictionary of Military and Associated Terms.

REFERENCES

Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011, as amended

Chairman of the Joint Chiefs of Staff Instruction 6510.05, "Department of Defense Cyber Red Teams," May 15, 2018[1]

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

Committee on National Security Systems Instruction No. 1001, "National Instruction on Classified Information Spillage," June 15, 2021

Committee on National Security Systems Instruction No. 1010, "Cyber Incident Response," September 27, 2021

Committee on National Security Systems Instruction No. 4009, "Committee on National Security Systems (CNSS) Glossary," March 2, 2022

Committee on National Security Systems Policy No. 18, "National Policy on Classified Information Spillage," May 19, 2021

Defense Federal Acquisition Regulation Supplement 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," current edition

DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007

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 5200.02, "DoD Personnel Security Program (PSP)," March 21, 2014, as amended

DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)," March 6, 2020

DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019, as amended

DoD Instruction 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013, as amended

DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022

DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016, as amended

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

DoD Instruction 8551.01, "Ports, Protocols, and Services Management (PPSM)," May 28, 2014, as amended

[1] Release via the internal Non-Classified Internet Protocol Router Network Chairman of the Joint Chiefs of Staff Directives Website through controlled access area is available only to .mil and .gov users. The Secret Internet Protocol Router Network access is unlimited.

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

DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended

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

DoD Manual 6025.18, "Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs," March 13, 2019

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

National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," April 16, 2018

National Institute of Standards and Technology Special Publication 800-40, "Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology," current edition

National Institute of Standards and Technology Special Publication 800-61, "Computer Security Incident Handling Guide," current edition

National Institute of Standards and Technology Special Publication 800-83, "Guide to Malware Incident Prevention and Handling for Desktops and Laptops," current edition

National Institute of Standards and Technology Special Publication 800-137A, "Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment," current edition

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