DoD Instruction 8530.03

Cyber Incident Response

Originating Component:	Office of the DoD Chief Information Officer
Effective:	August 9, 2023
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Approved by:	John B. Sherman, Chief Information Officer of Department of Defense

Purpose: In accordance with the authority in DoD Directive (DoDD) 5144.02, and pursuant to Subchapter II of Chapter 35 of Title 44, United States Code (U.S.C.), also known and referred to in this issuance as the "Federal Information Security Modernization Act of 2014" (FISMA); Section 2224 of Title 10, U.S.C.; and Parts 117 and 236 of Title 32, Code of Federal Regulations, this issuance establishes policy, assigns responsibilities, and provides procedures for DoD cyber incident response (CIR).

TABLE OF CONTENTS

TABLES

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) 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").

1.2. POLICY.

a. The DoD must:

(1) Prepare for future DoD CIR by establishing assets and capabilities to respond to cyber incidents and prevent cyber incidents by ensuring that all systems and system components (e.g., weapon systems, critical infrastructure information systems, or embedded processors supporting DoD missions) are sufficiently secure.

(2) Detect cyber incident(s) and analyze their operational and technical impact on DoD systems, system components, and supported missions.

(3) Contain cyber incident(s) to prevent further damage to DoD systems and system components and supported missions.

(4) Remediate, mitigate, or eliminate cyber incident(s) in DoD systems and system components to minimize impact to supported missions.

(5) Recover impacted DoD systems and system components.

(6) Provide DoD post-incident activities to prevent or lessen the impact of future cyber incidents.

(7) Assess and coordinate with the Department of Homeland Security (DHS) on cyber incidents involving controlled unclassified information (CUI) on defense industrial base (DIB) contractor networks.

b. DoD CIR will be performed by DoD Component-level organizations (e.g., DoD Component cyber command, network operations, and security centers or security operations centers) and supporting cybersecurity service providers (CSSP). The assigned DoD Component-level organizations will provide the required CIR services to their authorizing component.

SECTION 2: RESPONSIBILITIES

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

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

a. Develops and maintains DoD-level CIR policy consistent with:

(1) The National Cyber Incident Response Plan (NCIRP).

(2) The National Institute of Standards and Technology (NIST) cybersecurity framework.

(3) DoD Instructions (DoDI) 8500.01 and 8510.01.

b. Uses the Risk Management Framework (RMF) Technical Advisory Group and the RMF Knowledge Service (RMF KS) to provide CIR implementation guidance and procedures in coordination with:

(1) The United States Cyber Command (USCYBERCOM).

(2) Other designated DoD Components, when necessary.

c. Oversees the DoD Cyber Crime Center's (DC3) responsibility for DIB cyber incident reporting and response activity in accordance with DoDI 5205.13.

d. In coordination with the Under Secretary of Defense for Policy (USD(P)), shares cyber threat indicators (CTIs) and defensive measures within the DoD, pursuant to Subchapter I of Chapter 6 of Title 6, U.S.C., also known and referred to in this issuance as the "Cybersecurity Information Sharing Act of 2015."

e. Provides DoD Federal cybersecurity centers (FCCs) cybersecurity situational awareness for response coordination.

f. In coordination with the Director, Defense Information Systems Agency:

(1) Provides cybersecurity assessments to DoD Components.

(2) Offers validations for cybersecurity and security posture to DoD Components.

h. In coordination with the DoD Senior Agency Official for Privacy (SAOP), verifies that cyber incident reporting involving personally identifiable information (PII) occurs in accordance with Volume 2 of DoD Manual (DoDM) 5400.11, and cyber incident reporting involving electronic protected health information (ePHI) occurs in accordance with DoDI 8580.02 and DoDM 6025.18.

i. In coordination with the Commander, USCYBERCOM (CDRUSCYBERCOM), ensures that:

(1) Positions involved with CIR are appropriately identified.

(2) Personnel in those positions are appropriately qualified in accordance with DoDD 8140.01.

j. Leverages the Cyber Workforce Management Board as a mechanism to provide oversight to ensure CIR workforce management activities (e.g., identification, tracking, qualification, and professional development) are leveraged across DoD Components.

k. In coordination with the CDRUSCYBERCOM, assesses whether a major incident is resolved, and considers, in their assessment, whether:

(1) DoD has completed its incident response mission.

(2) The major incident is contained or eradicated.

(3) The Cyber Response Group (CRG) determines that a response is no longer required, or the Unified Coordination Group (UCG) is dissolved in accordance with Presidential Policy Directive (PPD)-41.

(4) The CDRUSCYBERCOM advises that a CIR is no longer necessary.

l. Notifies the USD(P) of cyber incidents affecting the operational status of defense critical assets (DCAs) and task critical assets (TCAs).

m. Coordinates with the CDRUSCYBERCOM and Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS) on cybersecurity active defense of the Department of Defense Information Network (DODIN).

2.2. DIRNSA/CHCSS.

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 CIO 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 2.7., the DIRNSA/CHCSS, in coordination with the DoD Chief Information Security Officer (CISO):

a. Provides oversight and guidance to ensure that DoD cyber threat analysis meets DoD Component operational and planning requirements for CIR.

b. Coordinates with the Directors, Defense Intelligence Agency (DIA) and the Defense Counterintelligence and Security Agency (DCSA) in activities that maintain active support to DoD CIR operations and activities.

c. Through the National Security Agency/Central Security Service (NSA/CSS) National Cybersecurity Operations Center (NCSOC) FCC coordinates with the Office of the Director of National Intelligence (ODNI) for major incident(s), in accordance with the NCIRP.

d. Provides attack sensing and warning to the OSD and DoD Components and populates databases with attack sensing and warning analysis.

e. Coordinates with the USD(P); the Director, DIA; and the Combatant Commanders, as mission owners, to ensure that cyber incidents affecting the operational status DCAs, TCAs, and mission assets are monitored and reported.

f. Coordinates activities of the NCSOC with other DoD Components to integrate NCSOC cyber threat reporting for the protection of national security systems.

g. Provides situational awareness (e.g., cyber threat, cyber incident, and analysis information) to enable integrated operational actions between FCCs.

h. Designates appropriate NSA/CSS senior officials to participate in the CRG.

i. Validates covered defense information (CDI) cyber incident reporting and incident reporting involving PII with the DC3 and CDRUSCYBERCOM.

j. Develops and maintains a CDI cyber incident response plan (CIRP) in coordination with the CDRUSCYBERCOM and the DoD SAOP for incidents involving PII in accordance with Volume 2 of DoDM 5400.11.

k. In coordination with CDRUSCYBERCOM, develops a CIR plan for national security systems.

l. Maintains NCSOC CIR strategic reporting in accordance with Paragraph 4.3.

2.3. USD(P).

In addition to the responsibilities in Paragraph 2.7., the USD(P):

a. Coordinates DoD Cyber UCG senior representative list activation.

b. Provides the DoD CISO with a list of DCAs and TCAs, updated annually.

c. Reviews DoD coordination responsibilities and procedures in support of the NCIRP for major cyber incidents with the CJCS:

(1) Every 4 years.

(2) If PPD-41, the NCIRP, or the cyber UCG concept of operations is updated.

(3) As necessary, based on lessons learned from:

(a) CIR exercises;

(b) CIR incidents; or

(c) Following participation in a cyber UCG.

d. Notifies the Assistant to the President for National Security Affairs (APNSA), and the Office of Management and Budget (OMB) of the DoD's evaluation and determination whether to adopt guidance issued in Department of Homeland Security Emergency Directives or Binding Operational Directives in accordance with Section 7, Paragraph j (iii) of Executive Order 14028.

2.4. ASSISTANT SECRETARY OF DEFENSE FOR SPACE POLICY.

Under the authority, direction, and control of the USD(P), the Assistant Secretary of Defense for Space Policy, in their role as the Principal Cyber Advisor of the Department of Defense in accordance with the April 4, 2022, Deputy Secretary of Defense Memorandum:

a. Serves as the principal civilian advisor for defense support to cyber incident response (DSCIR) and oversees the development and implementation of DSCIR capabilities.

b. Executes responsibilities for DSCIR, in accordance with Directive-type Memorandum (DTM) 17-007.

c. Serve as the Defense Domestic Crisis Manager and the Principal Cyber Advisor to the Secretary of Defense (SecDef).

d. Through the CRG:

(1) Designates DoD senior representatives to the Cyber UCG, in accordance with PPD- 41.

(2) Reviews major incidents received from the CDRCYBERCOM and notifies the CRG, or relevant members, when appropriate.

e. Provides guidance for using DoD Reserve Component personnel to support civilian law enforcement agencies during CIR.

2.5. UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT.

In addition to the responsibilities in Paragraph 2.7., the Under Secretary of Defense for Acquisition and Sustainment:

a. Develops policy and guidance for CIR of the DoD Acquisition and Sustainment Enterprise, and coordinates with:

(1) DC3 to develop situational awareness of CIR on unclassified DIB contractor networks.

(2) The Under Secretary of Defense for Intelligence and Security (USD(I&S)) to develop situational awareness on CIR intelligence activities associated with the DIB.

b. Establishes an asset to enable and execute mission-focused cyber hardening within the DoD Acquisition Enterprise to maintain economies of scale that might not be available to individual Service and agency acquisition enterprises in providing CIR-related remediation and mitigation services for DoD systems and system components.

c. Establishes the Supply Chain Risk Management Program and develops policy, guidance, and supporting tools that enable certified acquisition professionals to visualize and monitor program supply chains for probable activity by cyber adversaries that could lead to cybersecurity incidents and corresponding DoD CIR.

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

In addition to the responsibilities in Paragraph 2.7., the USD(R&E), through the DoD Damage Assessment Management Office (DAMO), coordinates with the following:

a. DC3 and the Military Department DAMOs for CIR damage assessments on unclassified contractor networks.

b. USD(I&S) on CIR intelligence activities.

2.7. DOD AND OSD COMPONENT HEADS.

The DoD and OSD Component heads:

a. Designate a lead DoD Component-level organization to coordinate, direct, and manage CIR activities. This designated organization will maintain a CIR reporting policy that details CIR reporting procedures for its organization in accordance with Sections 4 and 5.

b. Provide a minimum of one individual to the CJCS's DoD Cyber UCG senior representative list; individuals must:

(1) Be Senior Executive Service or general officer/flag officer. A General Schedule-15 may be delegated this role if a waiver is approved by the CJCS.

(2) Complete the currently approved National Incident Management System curriculum as published by the DoD CIO.

c. Develop, document, and disseminate a Component-level CIRP according to the DoD CIR process.

(1) Verify that subordinate organizations develop CIRPs, including guidance for their specific-level systems and system components, including the incorporation of any supporting commodity information technology service provider CIRPs as sub-plans to organizational plans:

(a) In accordance with RMF KS.

(b) Consistent with NIST Special Publication (SP) 800-61.

(c) Consistent with Volume 2 of DoDM 5400.11.

(2) Maintain the CIRP:

(a) Defines detailed reporting procedures at the Component level.

1. DoD Component-level organizations will report to the Joint Force Headquarters, DODIN (JFHQ-DODIN). The JFHQ-DODIN will report the NCSOC.

2. DoD Component-level organizations and below will **not** report to the following:

a. U.S. Computer Emergency Response Team (US-CERT); or

b. DHS National Cybersecurity and Communications Integration Center.

(b) Outlines training to personnel and organizations consistent with assigned roles and responsibilities for CIR, in coordination with USCYBERCOM, and in accordance with DoD Component guidance.

(c) Annotates the location and organizational ownership of interdependent systems and system components and identifies the assigned CSSP.

(d) Identifies vendor-provided services or assets (e.g., commercially hosted cloud environments or other provided services). The DoD Component must ensure that vendor responsibilities for CIR are clearly stated in contracts and service-level agreements.

(e) Points of contact for:

1. CIRP coordination with interdependent systems and system components.

2. Joint Strategic Planning Capabilities Plan specified coordination authority and supporting command joint cyber centers.

(f) Incorporates the:

1. JFHQ-DODIN Sector Framework to the component CIRP.

2. Mission-level Cyber Defense Plans for interdependent systems and system components supporting critical defense missions.

(g) Digital media logs associated with a cyber incident.

1. Verifies the digital media logs are accessible to authorized law enforcement and counterintelligence agencies and U.S. Intelligence Community as applicable.

2. Validates the integrity and validity of the digital media logs.

d. Plan for, coordinate, request, and support the deployment of USCYBERCOM CIR assets.

(1) Provide internal or external CIR support to assist system users and owners in reporting and responding to cyber incidents (e.g., help desks, cyber mission teams, and digital/multi-media (D/MM) forensic services).

(2) Establish relationships with CSSP(s) and identify CIR assets.

(3) Document CIR services provided by an external CSSP, to include:

(a) Specific DoD Component and external CSSP responsibilities, in accordance with DoDI 8530.01.

(b) Incident response security controls implementation using NIST SP 800-53.

(c) The RMF KS.

(4) Validate CIR assets to contact the component-appointed senior agency official for information security to assist with classification management determinations.

e. Direct the CIR intelligence support elements to provide all-source threat information for the organization's priority intelligence requirements.

(1) Identify processes and responsibilities for each coordinating CIR asset and support CSSP working with their appropriate intelligence support element to obtain and disseminate threat information and vulnerabilities.

(2) Perform follow-on reporting when significant patterns or intelligence data are identified with associated incidents or entity activity.

f. Provide operational reports to the OSD and the Joint Staff on costs (i.e., direct monetary or adverse effects on unit readiness) to resolve cybersecurity incidents. The reports should include an assessment, if applicable, of the costs to initially correct and maintain remediation and mitigation efforts for continued operations.

g. Provide information on DoD Component toolkits consisting of scripts, programs, and other resources used to safely acquire, examine, and preserve volatile and nonvolatile data from affected DoD systems and system components to share these assets with other DoD Component cyber incident responders.

h. Coordinate with USCYBERCOM, the DIA, and the NCSOC on cybersecurity incidents involving intelligence systems and system components.

i. Coordinate with USCYBERCOM, on implementing a CIR asset for shared awareness and reporting of cyber incidents involving PII on systems and system components in accordance with Volume 2 of DoDM 5400.11.

j. Coordinate with USCYBERCOM to determine cross-component dependency during incident prioritization.

k. Comply with standards, processes, and procedures established by the DoD Executive Agent (EA) for D/MM Forensics in support of CIR and maintain Component-level forensic training programs developed, implemented, and validated in coordination with the DoD EA for D/MM Forensics.

l. Maintain all CIR actions within unclassified non-DoD information systems and system components that process, store, or transmit unclassified non-public DoD information in accordance with DoDI 8582.01 to the extent provided by applicable contracts, grants, or other legal agreements with the DoD.

m. Coordinate with USCYBERCOM on the implementation of CIR assets.

n. Ensure all incidents that appear to be violations of Federal law are reported immediately upon identification to the appropriate defense criminal investigative organization or military department counterintelligence organization in accordance with DoDIs 8530.01, 5240.04, and O-5240.10.

2.8. SECRETARY OF THE AIR FORCE.

In addition to the responsibilities in Paragraph 2.7., the Secretary of the Air Force, as the DoD EA for D/MM Forensics and the DC3, through the Director, DC3:

a. Staffs and maintains the DC3 at the appropriate levels to fulfill its role as an FCC, in accordance with the NCIRP.

b. Serves as a single DoD focal point for receiving all cyber incident reporting related to unclassified contractor networks handling non-public DoD and Federal contract information and CUI.

(1) Maintains the cyber incident repository for unclassified DIB contractor networks handling contract information and CUI.

(2) Reports all DIB CDI cyber incidents involving the actual or suspected loss or compromise of:

(a) PII to the DoD SAOP in accordance with the May 6, 2019, Deputy SecDef Memorandum and Volume 2 of DoDM 5400.11.

(b) ePHI in accordance with DoDI 8580.02 and DoDM 6025.18.

(3) Conducts an assessment and immediately notifies the contracting officer and other U.S. Government stakeholders, as appropriate, upon receipt of a cyber incident report.

(4) Obtains malware associated with the DIB CDI cyber incident from the contractor for D/MM forensic analysis.

(5) Coordinates with DAMO on the damage assessment process.

c. As an FCC, the Director, DC3 provides updates to the CRG on the major incident(s) and measures being taken to resolve or respond to that incident, as required by the OSD CRG representative.

d. Provides focused analysis of and training for D/MM Forensics in accordance with DoDD 5505.13E.

(1) D/MM forensic analysis of malware and associated intrusion set data provided by:

(a) DoD Components.

(b) DIB contractors.

(c) Interagency activities.

(d) State and local governments.

(e) Specified private sector entities.

(2) Cyber-investigative and CIR training to:

(a) DoD personnel.

(b) As appropriate, other non-DoD government organizations.

e. In coordination with the USD(R&E) and the DoD CISO, develops, publishes, and maintains a DoD D/MM evidence handling guide which will:

(1) Be based on International Organization for Standardization/International Electrotechnical Commission 27037.

(2) Align policy with:

(a) All applicable DoD, NIST, and Committee on National Security Systems (CNSS) publications.

(b) FISMA data retention requirements.

f. In coordination with the USD(R&E) and the DoD CIO, develops, publishes, and maintains a DoD D/MM forensic guide, in accordance with NIST SP 800-86, which will:

(1) Include:

(a) Forensic roles and responsibilities.

(b) Monitoring and privacy.

(c) Data protection.

(d) Forensic training.

(e) Investigation acceleration procedures.

(f) Anonymity prevention.

(2) Validate that policy aligns with:

(a) The NCIRP.

(b) All applicable DoD, NIST, and CNSS publications.

g. Coordinates with the ODNI and the NCSOC for intelligence support for major incidents, in accordance with the NCIRP.

2.9. CHIEF, NATIONAL GUARD BUREAU.

In addition to the responsibilities in Paragraph 2.7., the Chief, National Guard Bureau, executes responsibilities for DSCIR, in accordance with DTM 17-007.

2.10. CJCS.

In addition to the responsibilities in Paragraph 2.7., the CJCS:

a. Maintains the DoD Cyber UCG senior representative list through the National Military Command Center.

b. Coordinates with the USD(P) to review DoD-significant cyber incident coordination responsibilities and procedures.

c. Executes responsibilities for DSCIR, in accordance with DTM 17-007.

2.11. CDRUSCYBERCOM.

In addition to the responsibilities in Paragraph 2.7., the CDRUSCYBERCOM:

a. Coordinates with assigned DoD and OSD Component CIR organizations.

b. Develops deployment plans and conducts deployment exercises with assigned DoD Component CIR organizations and supports CSSPs.

c. Pursuant to Section 167b of Title 10, U.S.C., sets cyber protection condition levels.

d. Trains and exercises CIR assets in coordination with assigned DoD and OSD Component CIR organizations.

e. Supports threat and asset CIR of the DODIN.

f. Analyzes incident reports determining whether a newly discovered and previously unknown vulnerability is identified for review by the vulnerabilities equities process in accordance with DoDI 8531.01.

g. Publishes DoD CIR orders and procedures (e.g., manuals) and, if unclassified, for posting on the RMF KS Website at https://rmfks.osd.mil/rmf/Pages/default.aspx.

h. Provides, as necessary, CIR reports (e.g., summaries, major cyber incidents and major cyber incidents involving PII, trends, enterprise-wide issues) to the following:

(1) OSD.

(2) Joint Staff.

(3) DoD CISO.

(4) DoD SAOP.

(5) DoD Components.

i. Maintains and disseminates the DoD intrusion detection system and DoD intrusion prevention system signature sets for DoD-level sensors through the JFHQ-DODIN.

j. Maintains an integrated capability of digital forensic analysts, cyber capability developers, and operational personnel to implement defensive measures to enable the DoD to respond to and deter cyber threats more effectively.

k. Identifies a set of scripts, programs, and other resources to safely acquire, examine, and preserve volatile and nonvolatile data from affected DoD systems or system components for use by assigned DoD and OSD Component CIR organizations.

l. For major incident reporting:

(1) Validates all cyber incident reports assessed to be major and, further, considers whether:

(a) The incident results in demonstrable harm to national security interests that require broader coordination for mitigation and response;

(b) An incident affecting the DoD has the potential to do demonstrable harm outside of the DODIN; or

(c) The DoD requires assistance from other departments or agencies to resolve or respond to the incident.

(2) Reports validated major cyber incidents not involving PII or ePHI within the DODIN— through the SecDef, the Deputy SecDef, and the Inspector General of the Department of Defense— to designated DoD congressional committees no later than:

(a) 7 days after the date the DoD determined that it has a reasonable basis to conclude that a major incident has occurred.

(b) 30 days after the initial notification. A report detailing the cyber incident and follow-on CIR will be prepared by USCYBERCOM, in coordination with:

1. The assigned OSD and DoD CIR organization that discovered the major incident.

2. Other appropriate DoD Components.

(c) Provides updates to the CRG on major incidents and measures being taken to resolve or respond to those incident(s), as required by the OSD CRG representative.

(3) Coordinates with the following:

(a) ODNI for intelligence in support of major incident response, in accordance with the NCIRP.

(b) The DC3 and the ODNI to complete cyber attribution analysis for incident prioritization for major incidents.

(4) Major incidents involving PII or ePHI will be handled in accordance with Volume 2 of DoDM 5400.11.

m. Develops and maintains a FISMA cyber incident record management policy and incident reporting program for all cyber incidents.

n. Sends a consolidated list every fiscal quarter of all validated cyber incidents where the confidentiality, integrity, or availability of the DODIN is compromised to DoD CISO.

o. Reports cyber incidents involving PII to the Cybersecurity and Infrastructure Security Agency (i.e., US-CERT) and the OMB Office of the Federal Chief Information Officer in accordance with Volume 2 of DoDM 5400.11.

SECTION 3: DOD CIR REPORTING

3.1. DOD AND OSD REPORTING REQUIREMENTS.

For all cyber incident reports:

a. Identify:

(1) Affected DoD and OSD Component(s).

(2) Category level of the incident.

(3) Current level of impact on component functions or services (i.e., functional impact).

(4) Type of information lost, compromised, or corrupted (i.e., information impact).

(5) Number of systems and system components, records, and users impacted.

(6) Network location of the observed activity.

(7) Priority of the incident.

(8) Attack vector(s) that led to the incident.

(9) When the activity was first detected.

(10) Point of contact information for additional follow-up.

b. Provide any:

(1) Indicators of compromise, including signatures or detection measures developed related to the incident.

(2) Mitigation activities undertaken in response to the incident.

c. Estimate the scope of time and resources needed to recover from the incident (i.e., recoverability).

3.2. DOD AND OSD REPORTING PROCEDURES.

DoD and OSD Components will not report cyber incidents to the US-CERT. Reporting requirements and metrics must be in accordance with Federal CIR guidelines. All organizations must report cyber incidents using these instructions:

a. Cyber Incidents.

(1) Report cyber incidents to the appropriate defense criminal investigative organization in accordance with Paragraph 2.7.

(2) Report national security systems and intelligence system cyber incidents in accordance with CNSS Instruction (CNSSI) 1010.

(3) Report the identified category and priority level as soon as possible. Components will provide updated information as it becomes available.

(4) Immediately report any incident meeting the definition of a "major incident" to USCYBERCOM for validation.

b. Cyber Incidents Involving PII.

(1) All DoD Components must treat each cyber incident involving PII as a breach in accordance with Volume 2 of DoDM 5400.11 and DoDM 6025.18 for ePHI.

(2) Any cyber incident(s) involving PII will be reported in accordance with Volume 2 of DoDM 5400.11 and DoDM 6025.18 for ePHI.

c. CDI Cyber Incident.

(1) Within 72 hours of discovery, report confirmed CDI cyber incident on cleared contractor classified systems and system components to the DCSA, and report confirmed CDI cyber breach on unclassified contractor systems and system components to the DC3. Additionally, report to the appropriate defense criminal investigative organization in accordance with Paragraph 2.7. immediately upon identification.

(2) In accordance with Defense Federal Acquisition Regulation Supplement Clause 252.204-7012, contractors or subcontractors must report cyber incidents that affect CDI or affect the contractor's ability to perform requirements designated as critical operations support. The contractor must conduct a review for evidence of compromise and rapidly report cyber incidents to the DoD, via an incident collection form, at https://dibnet.dod.mil.

d. Data Information Spillage Cyber Incident.

CNSS provides policy and instructions for CUI and classified data information spillage. All Components must follow the guidance provided in CNSS Policy 18 and the instructions provided in CNSSIs 1001 and 1010.

3.3. DOD COMPONENT LEVEL CIR ORGANIZATION REPORTING PROCEDURES.

All DoD Component-level CIR organizations must:

a. Send to USCYBERCOM a consolidated list every fiscal quarter of all cyber incidents in which the confidentiality, integrity, or availability of assigned systems and system components were compromised.

b. Report all incidents that appear to be violations of Federal law immediately upon identification to the appropriate defense criminal investigative organization in accordance with DoDI 8530.01.

c. Ensure reporting of cyber incidents involving PII occurs in accordance with Volume 2 of DoDM 5400.11.

d. Ensure ePHI reporting of cyber incidents involving PII occurs in accordance with Volume 2 of DoDM 5400.11 and DoDM 6025.18.

e. Upon receipt of CDI, verifiy and validate the CDI notification with the DCSA for contractor classified systems and DC3 for unclassified contractor systems.

f. Report cyber incidents involving national security systems and system components identified in the DoD Information Technology Portfolio Repository at https://ditpr.dod.mil/:

(1) In accordance with this issuance and USCYBERCOM guidance.

(2) Consistent with CNSSI 1010.

g. Verify and validate suspected major incidents.

h. Notify:

(1) USD(I&S) of classified information or CUI data spillage.

(2) DoD CISO, USD(P), and the USCYBERCOM of a suspected major incident(s) and provide advice on recommended defense, mitigation, and response options to address the incident(s).

(3) DCSA for cyber incidents related to cleared contractor classified systems and system components operating under the National Industrial Security Program, in accordance with Volume 1 of DoDM 5220.32 and Part 117 of Title 32, Code of Federal Regulations.

(4) DC3 for cyber incidents related to cleared contractor unclassified systems and system components in accordance with DoDI 5205.13, Part 236 of Title 32, Code of Federal Regulations, and the May 6, 2019, Deputy SecDef Memorandum.

(5) Component's Counter Insider Threat Program when the cyber incident was performed by an authorized system user in accordance with DoDD 5205.16.

SECTION 4: DOD CIR PROCESS

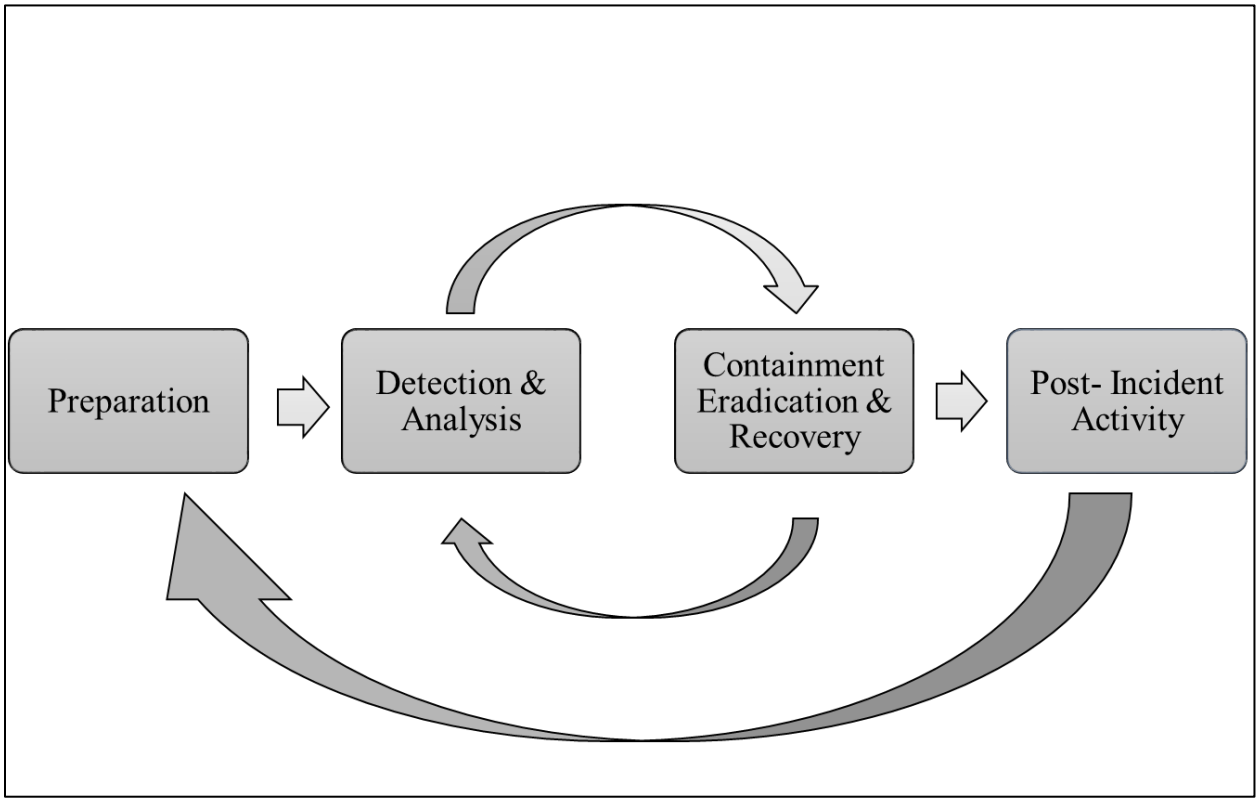
4.1. GENERAL.

a. The DoD CIR process is a four-phased, organized method to address and manage a cyber incident. (See Figure 1 for a visual representation of the four phases of the DoD CIR process.)

b. DoD and OSD Components, in coordination with the CSSPs and USCYBERCOM, will use the CIR process for CIR.

c. The DoD CIR process is a partnering effort with DoD force protection and mission assurance activities to support the overall joint protection function.

Figure 1. CIR Process



4.2. PREPARATION.

The assigned CIR organizations, in coordination with USCYBERCOM, will:

a. Develop CIRPs in accordance with:

(1) The DoD CIR process.

(2) Component mission and objectives.

(3) Annexes G and H of the NCIRP.

(4) CNSSI 1010.

b. Establish reporting procedures in accordance with Section 3.

(1) Maintain the reporting frequency to be in accordance with the DODIN risk assessment methodology (RAM).

(2) Verify that all CIR intelligence reporting procedures are in accordance with CJCS Manual 6510.01B.

(3) Use the DODIN RAM when evaluating reports to determine whether the incident(s):

(a) Meet the criteria of a major cyber incident; or

(b) Require interagency notification.

c. Establish CIR preparedness.

(1) Establish:

(a) Incident handler communications and facilities are appropriately equipped and maintained in accordance with applicable DoD standards and Federal regulations.

(b) Encryption software uses a validated Federal Information Processing Standard encryption algorithm.

(c) Incident analysis hardware and software (e.g., packet sniffers, D/MM forensic software, evidence-gathering accessories) are operational for incident handling procedures.

(b) Continuous monitoring assets (e.g., network-based and host-based intrusion detection and prevention systems and system components, antivirus software, log analyzers, intrusion detection systems, and system components, and security information and event management technologies) are correctly configured and operational.

(2) Provide incident:

(a) Analysis resources (e.g., port lists, network diagrams, cryptographic hashes) to response assets.

(b) Mitigation software to response assets.

(3) Configure network security to protect systems and system components from unauthorized access and activity in accordance with DoDI 8500.01.

(4) In accordance with DoDI 8531.01, verify that systems and system components comply with the DoD vulnerability management process.

(5) Use DODIN RAM guidelines to assess the risk to the system, subsystem, or system components.

4.3. DETECTION AND ANALYSIS.

The assigned CIR organizations, in coordination with USCYBERCOM and JFHQ-DODIN, will:

a. Identify the type of cyber incident and determine its attack vectors. (See Table 1 for additional information on attack vectors including types of attack vectors, a description, and examples of each.)

Table 1. Federal Agencies Attack Vector Taxonomy

Attack Vector	Description	Example
Unknown	The vector of the attack is unidentified.	This option is acceptable if the vector is unknown upon the initial report. The attack vector may be updated in a follow-up report.
Attrition	An attack employing brute force methods to compromise, degrade, or destroy systems and system components, networks, or services.	Denial of service intended to impair or deny access to an application—a brute force attack against an authentication mechanism (e.g., passwords or digital signatures).
Web	An attack executed from a website or web-based application.	A cross-site scripting attack is used to steal credentials or redirect a site that exploits a browser vulnerability and installs malware.
E-mail/Phishing	An attack is executed via an e-mail message or attachment.	Exploit code disguised as an attached document or a link to a malicious website in the body of an e-mail message.
External/Removable Media	An attack executed from removable media or a peripheral device.	Malware spreading onto a system from an infected flash drive.
Impersonation/Spoofing	An attack involving the replacement of legitimate content and services with a malicious substitute.	Spoofing, man-in-the-middle attacks, rogue wireless access points, and structured query language injection attacks all involve impersonation.

Table 1. Federal Agencies Attack Vector Taxonomy, Continued

Attack Vector	Description	Example
Improper Usage	Any incident resulting from the violation of an organization's acceptable usage policies by an authorized user, excluding the other categories.	User installs file-sharing software, leading to the loss of sensitive data, or a user performs illegal activities on a system.
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization.	A misplaced laptop or mobile device.
Other	An attack method that does not fit into any specific vector.	N/A

b. Identify precursors and indicators on attack vectors.

c. Collect data from automated detection assets and use secondary sources as necessary.

d. Perform initial impact analysis (e.g., profiling, performing incident correlation, running packet sniffers) and document findings.

e. Assess the incident impact on the system, subsystem, or system components in accordance with DODIN RAM guidelines.

f. Calculate the priority of the incident based on the contributing factors specified in this paragraph.

(1) Perform a functional impact assessment. (See Table 2 for the impact levels and their corresponding functional impacts.)

Table 2. Functional Impact Contributing Factor

Level	Functional Impact
1	No effect on the component's ability to provide service to all users.
2	Component mission essential services or functions are affected.
3	The component can still provide all critical services to all users but has lost efficiency.
4	The component has lost the ability to provide a critical service to a subset of system users.
5	The component can no longer provide some critical services to any users.
6	The component can no longer provide the most critical services to any users.
7	The component can no longer provide any critical services to any users.

(2) Determine the observed activity. Establish which category and objective is the most probable observed activity contributing factor in accordance with the ODNI cyber threat framework. (See Table 3 for additional information on observed activity contributing factors.)

Table 3. Observed Activity Contributing Factor

Category	Threat Action Objectives
Prepare	1. Plan activity. 2. Conduct research and analysis. 3. Develop resources and assets. 4. Acquire victim-specific knowledge. 5. Complete preparations.
Engage	1. Deploy an asset. 2. Interact with the intended victim. 3. Exploit vulnerabilities. 4. Deliver malicious capability.
Presence	1. Establish controlled access. 2. Hide. 3. Expand presence. 4. Refine the focus of the activity. 5. Establish persistence.
Effect/Consequence	1. Enable other operations. 2. Deny access. 3. Extract data. 4. Alter data and computer, network, or system behavior. 5. Destroy data.

(3) Determine the location of observed activity. Define where the observed activity occurred in the DoD systems, and system components. (See Table 4).

Table 4. Location of Observed Activity Contributing Factor

Level	Description
Level 0 – Unsuccessful	Existing network defenses repelled all observed activity.
Level 1 – Business Demilitarized Zone (DMZ)	The activity was observed in the business network's DMZ. These systems and system components are generally untrusted and are designed to be exposed to the Internet. Examples are a company's web server or e-mail server.
Level 2 – Business Network	The activity was observed in the business or corporate network of the victim. These systems and system components would be corporate user workstations, application servers, and other non-core management systems and system components.
Level 3 – Business Network Management	The activity was observed in business network management systems and system components (e.g., administrative user workstations, active directory servers, or other trust stores).
Level 4 – Critical System DMZ	The activity was observed in the DMZ that exists between the business network and a critical system network. These systems and system components may be internally facing services (e.g., SharePoint sites, financial systems, and system components, or relay "jump" boxes into more critical systems).
Level 5 – Critical System Management	The activity was observed in high-level critical systems and system components management (e.g., human-machine interfaces in industrial control systems).
Level 6 – Critical Systems	The activity was observed in the critical systems and system components that operate critical processes (e.g., programmable logic controllers in industrial control system environments, or aircraft flight control system).
Level 7 – Safety Systems	The activity was observed in critical safety systems and system components that maintain the safe operation of an environment. One example of a critical safety system is a fire suppression system.
Unknown	The activity was observed, but the network segment could not be identified.

(4) Determine, with a sufficient degree of certainty, an incident's origin and the responsible party in accordance with the best practices detailed in the ODNI Guide to Cyber Attribution.

(a) De-layer the judgment.

1. Provide the physical location where the incident most probably originated.

2. Identify the:

a. Most probable actors or groups involved.

b. Probable level of state responsibility for the incident. (See Table 5 for the levels of state responsibility and their definitions.)

Table 5. The Spectrum of State Responsibility

Status	Definition
State-prohibited	The national government will help stop third-party attacks.
State-prohibited-but-inadequate	The national government is cooperative but unable to stop the third-party attack.
State-ignored	The national government knows about the third-party attacks but is unwilling to take official action.
State-encouraged	Third parties control and conduct the attack, but the national government encourages them as a matter of policy.
State-shaped	Third parties control and conduct the attack, but the state provides some support.
State-coordinated	The national government coordinates third-party attackers by "suggesting" operational details.
State-ordered	The national government directs third-party proxies to conduct the attack on its behalf.
State-rogue-conducted	Out-of-control elements of the cyber forces of the national government conduct the attack.
State-executed	The national government conducts the attack using cyber forces under their direct control.
State-integrated	The national government attacks using integrated third-party proxies and government cyber forces.

(b) Determine the confidence level based on the following:

1. High Confidence.

The analyzed totality of evidence determines that the identified actor is **beyond a reasonable doubt with no reasonable alternative** the source of the incident.

2. Moderate Confidence.

The analyzed totality of evidence determines that the identified actor is **clearly and convincingly, with only circumstantial cases for alternatives**, the source of the incident.

3. Low Confidence.

The analyzed totality of evidence presents a **probable case** that the actor is the incident source, but there are **significant information gaps**.

(c) Determine the gaps: Identify a lack of sufficient data for a conclusion or declaration of confidence due to poor indicators.

(5) Use Table 6 to identify the information impact of the incident contributing factor. Categories are **not** mutually exclusive and DoD CIR assets can choose more than one.

Table 6. Information Impact Category of Incident Contributing Factor

Category	Type of Information Lost, Compromised, or Corrupted
No Impact	No known data impact.
Suspected But Not Identified	A data loss or impact to availability is suspected, but no direct confirmation exists.
Cyber Incident Involving Breach of PII	DoD data containing PII or ePHI was exposed, accessed, or extracted.
Proprietary Information	The confidentiality of unclassified proprietary information, such as protected critical infrastructure information, intellectual property, or trade secrets, was compromised.
Destruction Of Non-Critical Systems	Destructive techniques, such as master boot record overwrite, have been used against a non-critical system.
Critical Systems Data Infiltration	Data pertaining to a critical system has been exfiltrated.
Core Credential Compromise	Core system credentials (such as domain or enterprise administrative credentials) or credentials for critical systems and system components have been exfiltrated.
Destruction Of Critical System	Destructive techniques, such as Master Boot Record overwrite, have been used against a critical system.
Data Spillage	Classified or CUI is inadvertently placed on information systems and system components not authorized to process such information.

(6) Use Table 7 to categorize how quickly the affected system and system components will take to recover.

Table 7. Recoverability Contributing Factor

Category	Definition
Regular	The time to recover is predictable with existing resources.
Supplemented	Time to recover is predictable with additional resources.
Extended	Time to recovery is unpredictable; additional resources and outside help are required.
Not Recoverable	Recovery from the incident is impossible (e.g., categories of CUI, PII, ePHl, personal information, or classified information exfiltrated and posted publicly). In such a case, launch an investigation.

(7) Determine cross-component dependency. Cross-component dependency is a weighted factor based on how the affected system, systems, or components depend on the DODIN. The JFHQ-DODIN determines this in coordination with the USCYBERCOM.

(8) Determine the potential impact. Potential impact measures the overall effect of the complete loss of service to the impacted component. Depending on what system, subsystem, or system component is affected, incidents can affect different critical infrastructure assets differently. Components should calculate weighted factors based on available statistics. The calculated potential impact is treated as the best estimate in priority response to incidents.

g. Prioritize the incident and determine the incident priority, in accordance with the cyber incident severity schema detailed in Table 8. "High," "Severe," and "Emergency" categories are always major incidents, in accordance with OMB Memorandum M-18-02.

Table 8. Cyber Incident Severity Schema

Level	Priority	Definition
Level 0	Baseline–Negligible (White)	A baseline incident–the negligible-priority incident is an incident that is **highly unlikely to result** in demonstrable harm to national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.
	Baseline–Minor (Blue)	A baseline incident–the minor-priority incident is an incident that is **highly unlikely to result** in demonstrable harm to national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. **The potential for impact, however, exists and warrants additional scrutiny.**
Level 1	Low (Green)	A low-priority incident is **unlikely to result** in demonstrable harm to national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. Mission functions are **not** significantly affected. Alternate modes of operations are available.
Level 2	Medium (Yellow)	A medium-priority incident **may result** in demonstrable harm to national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people**. There is a significant adverse effect on the component's mission.**
Level 3	High (Orange)	A high-priority incident is **likely to result** in demonstrable harm to national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.
Level 4	Severe (Red)	A severe-priority incident **is likely to result in a significant impact** on national security interests, foreign relations, or the economy of the United States or public confidence, civil liberties, or public health and safety of the American people.
Level 5	Emergency (Black)	An emergency-priority incident poses an **imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of U.S. persons.**

h. Implement an incident-reporting policy.

4.4. CONTAINMENT, ERADICATION, AND RECOVERY.

The assigned CIR organizations in coordination with USCYBERCOM will:

a. Perform Containment.

(1) Choose a Containment Strategy.

Use the criteria in Paragraph 4.4.a.(1)(c) to assist in determining which is appropriate.

(a) Containment strategies vary based on the type of incident (e.g., malicious cyber-attack, a breach involving PII, data exfiltration, information data spillage).

(b) Create individual containment strategies for each major incident type.

(c) Appropriate containment strategy criteria include:

1. Potential theft or damage to resources and assets.

2. Evidence preservation requirements.

3. Service availability (e.g., network connectivity, services provided to external parties).

4. Time and resources required for implementation.

5. Strategy effectiveness (partial or full containment).

6. Solution duration (e.g., emergency, temporary, permanent).

(2) D/MM Evidence Identification, Collection, Acquisition, and Preservation.

The DoD Components will handle evidence associated with cyber incidents in accordance with the evidence handling procedures developed pursuant to Paragraph 2.8.f. When the forensic capabilities of the DoD Component cannot identify the attacking hosts, the Component should leverage the DoD EA for D/MM Forensics through the DC3.

(3) Identify the Attacking Hosts.

Perform forensic, active, or manual identification after containment stops the spread of the cyber incident.

b. Perform Eradication.

(1) Eliminate the incident's components (e.g., delete malware, disable cyber-breached user accounts).

(2) Identify and mitigate exploited vulnerabilities in accordance with DoDI 8531.01.

c. Perform recovery.

(1) Restore systems and system components to regular operations.

(2) Confirm that systems and system components usually function.

(3) Remediate vulnerabilities to prevent similar incidents, in accordance with DoDI 8531.01.

(4) If applicable:

(a) Restore systems and system components from clean backups.

(b) Rebuild systems and system components from scratch.

(c) Replace compromised files with clean versions.

(d) Install patches.

(e) Change passwords.

(f) Tighten network perimeter security.

(5) Implement operating system- or application-specific recovery actions in accordance with the manufacturer's instructions.

4.5. POST-INCIDENT ACTIVITY.

The assigned CIR organizations in coordination with USCYBERCOM will:

a. Collect incident lessons learned.

b. If necessary, modify the security policy and awareness program based on lessons learned.

c. Reconfigure software to:

(1) Support security policy changes; or

(2) Comply with existing policy.

d. Deploy additional malware detection software, if necessary.

e. Reconfigure malware detection software (e.g., increase frequency, accuracy, scope, update distribution efficiency, or take other appropriate actions in response to detected malware).

f. Collect incident data. Use actionable data metrics to improve on existing policies and procedures. Collected incident data actionable metrics include:

(1) Number of incidents handled.

(2) Total time per incident.

(3) Asset response time.

(4) Report times.

(5) Objective assessment of each incident.

(6) Number of assets required for response.

(7) Recorded precursors and identifiers.

(8) Monetary damage.

(9) Vector of attack per incident.

(10) Vulnerabilities exploited.

(11) Incident reoccurrence.

(12) Initial impact assessment and final impact assessment differential.

(13) Possible preventative measures.

g. Perform D/MM forensic examination and analysis.

(1) Follow procedures in accordance with NIST SP 800-86 and the DC3 DoD D/MM forensic guide upon its publication in accordance with Paragraph 2.8.f., as applicable.

(2) Validate forensic examination and analysis pursuant to State and Federal legal requirements.

h. Ensure DoD's Breach Response Plan is executed in the event of cyber incidents involving PII or ePHI in accordance with Volume 2 of DoDM 5400.11.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
CDI	covered defense information
CDRUSCYBERCOM	Commander, United States Cyber Command
CIR	cyber incident response
CIRP	cyber incident response plan
CJCS	Chairman of the Joint Chiefs of Staff
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems instruction
CRG	cyber response group
CSSP	cybersecurity service provider
CTI	cyber threat indicator
CUI	controlled unclassified information
DAMO	Damage Assessment Management Office
DC3	DoD Cyber Crime Center
DCA	defense critical asset
DCSA	Defense Counterintelligence and Security Agency
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIB	defense industrial base
DIRNSA/CHSS	Director, National Security Agency/Chief, Central Security Service
D/MM	digital/multi-media
DMZ	demilitarized zone
DoD CIO	DoD Chief Information Officer
DoD CISO	DoD Chief Information Security Officer
DoDD	DoD directive
DoDI	DoD instruction
DODIN	Department of Defense information network
DoDM	DoD manual
DSCIR	defense support to cyber incident response
DTM	directive-type memorandum
EA	executive agent
ePHI	electronic protected health information
FCC	Federal cybersecurity center
FISMA	Federal Information Security Modernization Act of 2014

ACRONYM	MEANING
GS	general schedule
JFHQ-DODIN	Joint Force Headquarters, Department of Defense Information Network
N/A	not applicable
NCIRP	national cyber incident response plan
NCSOC	National Security Agency/Central Security Service National Cybersecurity Operations Center
NIST	National Institute of Standards and Technology
NSA/CSS	National Security Agency/Central Security Service
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
PII	personally identifiable information
PPD	Presidential policy directive
RAM	risk assessment methodology
RMF	risk management framework
RMF KS	Risk Management Framework Knowledge Service
SAOP	Senior Agency Official for Privacy
SecDef	Secretary of Defense
SP	special publication
TCA	task critical asset
UCG	Unified Coordination Group
U.S.C.	United States Code
US-CERT	U.S. Computer Emergency Response Team
USCYBERCOM	United States Cyber Command
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P)	Under Secretary of Defense for Policy
USD(R&E)	Under Secretary of Defense for Research and Engineering

G.2. DEFINITIONS.

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

TERM	DEFINITION
anonymity prevention	The prevention of the process or processes a cyber threat uses to attain anonymity to its target. For example, the deciphering of cloaking algorithms for location-based services.
asset	Defined in CNSSI 4009.
attack sensing and warning	Defined in CNSSI 4009.
breach	Defined in OMB Memorandum M-17-12.
brute force attack	A cryptographic attack that involves trying all possible combinations to find a match.
capability	An asset that is developed over time by an organization to accomplish its goal or mission (e.g., a team, skill set, or program).
CDI	Unclassified controlled technical information or other information as described in the CUI Registry that requires safeguarding and dissemination controls **and is either:** Marked or otherwise identified in the contract and provided to the contractor by DoD in support of the performance of the contract; **or** Collected, developed, received, transmitted, used, or stored by the contractor in the performance of the contract.
CIR	A cybersecurity method to minimize possible impacts of cybersecurity incidents and assist in identifying, classifying, responding, and reporting cybersecurity incidents related to critical cyber assets.
counterintelligence	Defined in the DoD Dictionary of Military and Associated Terms.
CRG	Defined in PPD-41.
CSSP	Defined in DoDI 8530.01.
CTI	Defined in the Cybersecurity and Information Sharing Act of 2015.

TERM	DEFINITION
cyber	Defined in Volume 2 of NIST Interagency Report 8074.
cyber incident	Defined in Federal Information Processing Standards Publication 200 as "incident."
cybersecurity active defense	Aggressive interdiction and disruption efforts to thwart an attack involving computers and networks. This includes interceding and disrupting an attack or a threat's preparation to attack, either pre-emptively or in self-defense.
cybersecurity service	Defined in DoDI 8530.01.
defensive measure	Defined in the Cybersecurity and Information Sharing Act of 2015.
DoD CISO	The official responsible for carrying out the DoD CIO responsibilities under FISMA and serving as the DoD CIO's primary liaison to the agency's authorizing officials, information system owners, and information system security officers pursuant to Section 3554 of Title 44, U.S.C.
DODIN	Defined in the DoD Dictionary of Military and Associated Terms.
DODIN operations	Defined in the DoD Dictionary of Military and Associated Terms.
economy of scale	A proportionate saving in costs gained by an increased level of production.
ePHI	Defined in DoDI 8580.02.
event	Any observable occurrence in an information system.
follow up report	Report submitted to provide amended or additional information about an event that has already been reported, mainly if the event was severe and unexpected.
hardware	Defined in CNSSI 4009.
incident	Defined in OMB Memorandum M-17-12.
indicator	Defined in CNSSI 4009.
information impact	The assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability of an information type.

TERM	DEFINITION
information technology	Defined in CNSSI 4009.
jump box	System on a network used to access and manage devices in a separate security zone. A jump box is a hardened and monitored device that spans two different security zones and provides controlled access between them.
major incident	Defined in OMB's annual guidance memorandum on Federal Information Security and Privacy Management Requirements. At the time of this publication, it is OMB Memorandum M-23-03. Pursuant to PPD-41, if an incident is a major incident, it is also a "significant cyber incident." A major incident will also trigger the coordination mechanisms outlined in PPD-41 and potentially require participation and actions from a Cyber UCG.
malware	Malicious code or malicious logic
manual identification	Manually identifying infected hosts on a server.
mission	Defined in the DoD Dictionary of Military and Associated Terms.
national security system	Defined in CNSSI 4009.
observed activity	The information known about the threat actor on the network.
PII	Defined in OMB Circular A-130.
precursor	Defined in CNSSI 4009.
resource	An asset is acquired by an organization to accomplish its goal or mission (e.g., equipment).
significant cyber incident	Defined in PPD-41.
software	Defined in CNSSI 4009.
spillage	A cyber incident where either classified or sensitive information is inadvertently placed on information systems that are not authorized to process such data.

TERM	DEFINITION
subsystem	Defined in NIST SP 800-37.
system	Defined in CNSSI 4009.
system component	Defined in NIST SP 800-171.

REFERENCES

Chairman of the Joint Chiefs of Staff Manual 6510.01B, "Cyber Incident Handling Program," current edition

Code of Federal Regulations, Title 32

Committee on National Security Systems Instruction 1001, "(U) National Instruction on Classified Information Spillage," June 2021

Committee on National Security Systems Instruction 1010, "(U) Cyber Incident Response," September 2021

Committee on National Security Systems Instruction 4009, "Committee on National Security Systems (CNSS) Glossary," March 2, 2022

Committee on National Security Systems Policy 18, "National Policy for Classified Information Spillage," May 19, 2021

Defense Federal Acquisition Regulation Supplement, Clause 252.204-7012, current edition

Department of Homeland Security, "National Cyber Incident Response Plan," December 2016

Department of Defense Information Networks, "Risk Assessment Methodology Guideline," October 2017, as amended[1]

Deputy Secretary of Defense Memorandum, "Defense Industrial Base Cyber Incident Notification Process," May 6, 2019

Deputy Secretary of Defense Memorandum, "Designation of the Department of Defense Principal Cyber Advisor," April 4, 2022

Directive-type Memorandum 17-007, "Interim Policy and Guidance for Defense Support to Cyber Incident Response," June 21, 2017, as amended

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014, as amended

DoD Directive 5505.13E, "DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)," March 1, 2010, as amended

DoD Directive 8140.01, "Cyberspace Workforce Management," October 5, 2020

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

DoD Instruction 5240.04, "Counterintelligence (CI) Investigations," April 1, 2016, as amended

DoD Instruction O-5240.10, "Counterintelligence (CI) in the DoD Components," April 27, 2020

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

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

[1] This reference is available to authorized users at https://intelshare.intelink.gov/sites/uscybercom/CWL/USCYBERCOMDocuments/DoD_Information_Networks_Risk_Assessment_Methodology_v2.1.pdf

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 8580.02, "Security of Individually Identifiable Health Information in DoD Health Care Programs," August 12, 2015

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

DoD Manual 5220.32, Volume 1, "National Industrial Security Program: Industrial Security Procedures for Government Activities," August 1, 2018, 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

Executive Order 14028, "Improving the Nation's Cybersecurity," May 12, 2021

Federal Emergency Management Agency, "National Incident Management System," current edition

Federal Information Processing Standards Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006

International Organization for Standardization/International Electrotechnical Commission 27037, "Information Technology – Security Techniques – Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence," October 2012

National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," April 16, 2018

National Institute of Standards and Technology Interagency Report 8074, Volume 2, "Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity," December 2015

National Institute of Standards and Technology Special Publication 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," December 2018

National Institute of Standards and Technology Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," September 2020, as amended

National Institute of Standards and Technology Special Publication 800-61, Revision 2, "Computer Security Incident Handling Guide," August 2012

National Institute of Standards and Technology Special Publication 800-86, "Guide to Integrating Forensic Techniques into Incident Response," August 2006

National Institute of Standards and Technology Special Publication 800-171, Revision 2, "Protecting Controlled Unclassified Information on Nonfederal Systems and Organizations," February 2020, as amended

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

Office of the Director of National Intelligence, "A Guide to Cyber Attribution," September 14, 2018

Office of Management and Budget Circular A-130, "Management of Federal Information Resources," July 28, 2016

Office of Management and Budget Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," January 3, 2017

Office of Management and Budget Memorandum M-18-02, "Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements," October 16, 2017

Office of Management and Budget Memorandum M-23-03, "Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements," December 2, 2022

Presidential Policy Directive 41, "United States Cyber Incident Coordination," July 26, 2016

United States Code, Title 6, Chapter 6, Subchapter I (also known and referred to as the "Cybersecurity Information Sharing Act of 2015")

United States Code, Title 10

United States Code, Title 32

United States Code, Title 44, Subchapter III of Chapter 35 (also known as the "Federal Information Security Modernization Act of 2014")