DoD Instruction 8582.01

Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information

Originating Component:	Office of the Chief Information Officer of the Department of Defense
Effective:	December 9, 2019
Releasability:	Cleared for public release. Available on the DoD Issuances Website at http://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems," June 6, 2012
Approved by:	Dana Deasy, DoD Chief Information Officer

Purpose: In accordance with the authority in DoD Directive (DoDD) 5144.02, this issuance establishes policy, assigns responsibilities, and provides direction for managing the security of non-DoD information systems that process, store, or transmit unclassified nonpublic DoD information, including controlled unclassified information (CUI).

TABLE OF CONTENTS

TABLES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance:

a. Applies to:

(1) 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 the 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").

(2) All unclassified non-DoD information systems to the extent provided by applicable contracts, grants, or other legal agreements with the DoD that process, store, or transmit unclassified nonpublic DoD information. This includes unclassified non-DoD information systems operated by mission partners.

b. Does **not** apply to:

(1) DoD information systems operated by a contractor or other entity on behalf of the DoD as described in DoD Instruction (DoDI) 8510.01. Such information systems are treated the same as those operated by a DoD organization.

(2) Non-DoD information systems providing information technology services to the DoD. Such information systems follow the guidance prescribed in DoDIs 8500.01 and 8510.01.

(3) Unclassified DoD information that has been cleared for public release in accordance with DoDD 5230.09.

1.2. POLICY. It is DoD policy that non-DoD information systems provide adequate security for all unclassified nonpublic DoD information. Appropriate requirements must be incorporated into all contracts, grants, and other legal agreements with non-DoD entities, including memorandums of agreement established in accordance with DoDI 4000.19.

SECTION 2: RESPONSIBILITIES

2.1. DOD CHIEF INFORMATION OFFICER (CIO). In addition to the responsibilities in Paragraph 2.5., the DoD CIO:

a. Assigns the DoD Senior Information Security Officer to oversee implementation of this issuance in coordination with the Under Secretary of Defense for Intelligence (USD(I)), the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), and the Under Secretary of Defense for Research and Engineering (USD(R&E)), as appropriate.

b. Oversees integration of this guidance into Defense Industrial Base (DIB) cybersecurity activities in accordance with DoDI 5205.13.

c. In coordination with the USD(A&S) and the USD(R&E), identifies, develops, and implements the DoD acquisition contracting process, policy, and procedures for improved protection of unclassified DIB information systems where unclassified non-public DoD information is processed, stored, or transmitted on unclassified DIB information systems, to include:

(1) Subsection 52.204-21 of the Federal Acquisition Regulation (FAR).

(2) Subsection 252.204-7012 of the Defense Federal Acquisition Regulation Supplement (DFARS).

d. In coordination with the USD(R&E) and the USD(A&S), engages the DIB to identify and validate best practices to improve protection of nonpublic unclassified DoD information developed, used, and shared by non-DoD entities in support of defense acquisition programs.

e. Requires non-DoD unclassified information systems containing CUI meet the security requirements of Part 2002 of Title 32, Code of Federal Regulations and DoD CUI policy in coordination with the USD(I).

2.2. USD(A&S). In addition to the responsibilities in Paragraph 2.5., the USD(A&S):

a. In coordination with the USD(I), the USD(R&E), the DoD CIO, and the DoD Components, as appropriate, identifies, develops, and implements the acquisition regulations, policies, and procedures for improved protection of contractor information systems processing, storing, or transmitting unclassified DoD information that has not been publicly released.

b. In coordination with the USD(I), the USD(R&E), and the DoD CIO, engages the DIB to identify and validate best practices to improve protection of nonpublic unclassified DoD information developed, used, and shared by non-DoD entities in support of defense acquisition programs.

2.3. USD(R&E). In addition to the responsibilities in Paragraph 2.5., the USD(R&E):

a. In coordination with the DoD CIO and the USD(A&S), engages the DIB to identify and validate best practices to improve protection of nonpublic unclassified DoD information developed, used, and shared by non-DoD entities in support of defense acquisition programs.

b. Develops cyber incident damage assessment policy and oversees the process to conduct assessments of DoD programs, as required, on unauthorized access and compromise of DIB information systems containing unclassified DoD information.

2.4. USD(I). As the DoD Senior Agency Official for Security, the USD(I), in addition to the responsibilities in Paragraph 2.5., in coordination with the DoD CIO, the USD(A&S), and the USD(R&E), as appropriate:

a. Oversees implementation of this issuance in areas of USD(I) responsibility.

b. Ensures information security requirements for CUI contained on non-DoD information systems are in accordance with DoD CUI policy.

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

a. Require contracts, grants, or other legal agreements to protect:

(1) Unclassified nonpublic DoD information provided to, or developed by, non-DoD entities in support of DoD activities according to the basic information system safeguards in Table 1 (see Section 3).

(2) DoD CUI provided to, or developed by, non-DoD entities in support of DoD activities according to the DoD CUI information system safeguards described in Paragraph 3.2.b.

b. In addition to the safeguards specified in Section 3, require contracts, grants, and other legal agreements, by the insertion of applicable language, to implement any unique protection measures or reporting requirements regarding compromise, loss, or unauthorized disclosure of DoD CUI required by law, regulation, or government-wide policy (e.g., those relating to privacy, health information, law enforcement, or export control).

c. In accordance with the authority in DoDD 5505.13E, ensure the DoD Cyber Crime Center (DC3) is identified as the single focal point for receiving cyber incident reports from non-DoD entities regarding unclassified information systems of non-DoD entities that process, store, or transmit DoD CUI as described in Paragraph 3.3. Cyber incidents include activities taken through the use of information systems that result in a compromise or an actual or potentially adverse effect on an information system or the information residing therein.

SECTION 3: PROCEDURES

3.1. GENERAL. Unclassified nonpublic DoD information may be disseminated by the contractor, grantee, or awardee to further the contract, grant, or agreement objectives, provided the information is disseminated within the scope of assigned duties, is not otherwise restricted by the contract, grant or agreement, and with a clear expectation that confidentiality will be preserved. Examples are:

a. Nonpublic information provided to a contractor (e.g., with a request for proposal).

b. Information developed during the course of a contract, grant, or other legal agreement (e.g., draft documents, reports, or briefings and deliverables).

c. Privileged information contained in transactions (e.g., privileged contract information, program schedules, or contract-related event tracking).

3.2. INFORMATION SYSTEM SAFEGUARDS. Adequate security will vary depending on the nature and sensitivity of the information on any given non-DoD information system.

a. All non-DoD information systems that process, store, or transmit unclassified nonpublic DoD information must be safeguarded in accordance with the basic safeguarding requirements in Table 1. These requirements must be included in contracts, grants, and other legal agreements (in contracts, these are implemented in accordance with FAR 52.204-21.

b. Non-DoD information systems processing, storing, or transmitting DoD CUI must be protected in accordance with National Institute of Standards and Technology Special Publication (NIST SP) 800-171. If the non-DoD entity intends to use an external cloud service provider to process, store, or transmit any DoD CUI in performance of contracts, grants, or other legal agreements; the non-DoD entity must require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program Moderate baseline (https://www.fedramp.gov/resources/documents/).

(1) This is typically implemented contractually in accordance with DFARS 252.204-7012.

(2) DoD Components should restrict their security requirements to NIST SP 800-171 for information systems processing, storing, or transmitting DoD CUI unless the authorizing law, regulation, or Government-wide policy for the CUI category of the information involved prescribes specific safeguarding requirements for protecting the information's confidentiality, or there is a specific documented need to increase security above the Federal Information Processing Standards Publication 199 moderate impact level.

c. Non-DoD entities meeting the Basic Safeguarding Requirements in Table 1, meet the comparable security requirements of the NIST SP 800-171 as indicated.

Table 1. Basic Safeguarding Requirements

BASIC SAFEGUARDING REQUIREMENT	NIST SP 800-171 REQUIREMENT
Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)	3.1.1
Limit information system access to the types of transactions and functions that authorized users are permitted to execute	3.1.2
Verify and control/limit connections to, and use of, external information systems	3.1.20
Control information posted or processed on publicly accessible information systems	3.1.22
Identify information system users, processes acting on behalf of users, or devices	3.5.1
Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems	3.5.2
Sanitize or destroy information system media containing nonpublic DoD information before disposal or release for reuse	3.8.3
Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals	3.10.1
Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices	3.10.3, 3.10.4, and 3.10.5
Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems	3.13.1
Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks	3.13.5
Identify, report, and correct information and information system flaws in a timely manner	3.14.1
Provide protection from malicious code at appropriate locations within organizational information systems	3.14.2
Update malicious code protection mechanisms when new releases are available	3.14.4
Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed	3.14.5

3.3. CYBER INCIDENT REPORTING AND RESPONSE. In accordance with DoD's DIB Cyber Security Activities Federal Rule, Part 236 of Title 32, Code of Federal Regulations, DoD Components must, through relevant contracts or other agreements, require non-DoD entities to report and respond to cyber incidents affecting their information systems that process, store, or

transmit DoD CUI as specified in the following subparagraphs. This is typically implemented contractually in accordance with DFARS 252.204-7012.

a. Cyber Incident Reporting Requirement.

(1) When a non-DoD entity discovers a cyber incident, the non-DoD entity must conduct a review for evidence of compromise of DoD CUI. The review should include analyzing the non-DoD entity's information system(s) that were part of the cyber incident, including, but not limited to, identifying compromised computers, servers, specific data, user accounts, and other information systems on the non-DoD entity's network(s) that may have been accessed as a result of the cyber incident, in order to identify compromised DoD CUI and report cyber incidents to DoD.

(2) The non-DoD entity will rapidly report (within 72-hours of discovery) all cyber incidents affecting DoD CUI on unclassified information systems through the web portal at https://dibnet.dod.mil. Upon receipt, DC3 will provide a copy of the report to the appropriate contracting officer or designated government representative.

b. Medium Assurance Certificate Requirement. The non-DoD entity must have or acquire a DoD-approved medium assurance certificate to report cyber incidents. Information on obtaining a DoD-approved medium assurance public key infrastructure certificate can be found on the External Certification Authority Program Website at https://iase.disa.mil/pki/eca/Pages/index.aspx

c. Malicious Software Requirement. When the non-DoD entity discovers and isolates malicious software (also referred to as malicious code) in connection with a reported cyber incident, the non-DoD entity must submit the malicious software to the DC3 in accordance with instructions provided by DC3 or the contracting officer.

d. Media Preservation and Protection Requirement. When a non-DoD entity discovers a cyber incident has occurred, the non-DoD entity must preserve and protect images of all known affected information systems and all relevant monitoring and packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest through DoD processes established by the USD(R&E).

e. Access for Forensic Analysis Requirement. Upon request from a DoD Component, the non-DoD entity must provide DoD access to additional information or equipment that is necessary to conduct a forensic analysis.

f. Cyber Incident Damage Assessment Requirement. If the DoD Component elects to conduct a damage assessment, the DoD Component will, following processes established by the USD(R&E), request that the non-DoD entity provide all of the damage assessment information gathered in accordance with Paragraph 3.3.d.

g. DoD Safeguarding and Use of Non-DoD Entity Attributional or Proprietary Information. DoD Components will protect against unauthorized use or release of information obtained from the non-DoD entity (or derived from information obtained from the non-DoD

entity) that contains non-DoD entity attributional or proprietary information, including such information submitted in accordance with Paragraph 3.3.a.

3.4. VALIDATION AND COMPLIANCE.

a. When warranted based on the criticality of the information provided to, or developed by, the non-DoD entity, DoD Components will include a requirement in the solicitation for the non-DoD entity to describe implementation of the requirements of NIST SP 800-171, and as appropriate, include a requirement for the non-DoD entity to demonstrate compliance before or upon award of the contract, grant, or execution of another legal agreement. The DoD Component may include a requirement in the solicitation for the non-DoD entity to notify the DoD Component when there is a deficiency that affects DoD information, or to periodically review how they are resolving deficiencies and meeting requirements, or both. Additionally, for contracts that include the clause at DFARS 252.204-7012, the DoD Component's contracting officer may request the contractor for an assessment of the contractor's compliance with the requirements of that clause upon receipt of a cyber incident report.

b. DoD Components should not intrude into the operations, maintenance, or governance of the non-DoD entity's internal information system by specifying the content and format of plans of action that address deficiencies, or specifying the parameters of security controls.

GLOSSARY

G.1. ACRONYMS.

CIO	chief information officer
CNSSI	Committee on National Security Systems instruction
CUI	controlled unclassified information
DC3	DoD Cyber Crime Center
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DoDD	DoD directive
DoDI	DoD instruction
FAR	Federal Acquisition Regulation
NIST SP	National Institute of Standards and Technology Special Publication
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I)	Under Secretary of Defense for Intelligence
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.

adequate security. Defined in Committee on National Security Systems Instruction (CNSSI) 4009.

compromise. Defined in CNSSI 4009.

non-DoD entity attributional/proprietary information. Information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

CUI. Defined in Volume 4 of DoD Manual 5200.01.

controlled technical information. Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in

DoDI 5230.24. The term does not include information that is lawfully publicly available without restrictions.

cyber incident. Actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

DoD CUI. CUI that is marked or otherwise identified and provided to a non-DoD entity by or on behalf of DoD in support of the performance of a contract, grant or other legal agreement; or collected, developed, received, transmitted, used, or stored by or on behalf of the non-DoD entity in support of the performance of the contract, grant or other legal agreement.

DoD information. Any information that is in DoD custody and control; relates to information in DoD custody and control; was acquired by DoD employees as part of their official duties or because of their official status within DoD, including information that is provided by the DoD to a non-DoD entity; or is developed by a non-DoD entity in support of an official DoD activity.

DIB. Defined in the DoD Dictionary of Military and Associated Terms.

federal contract information. Defined in FAR 52.204-21. An example of nonpublic DoD information when it relates to a DoD contract.

IT service. Defined in DoDI 8500.01.

malicious code. Defined in CNSSI 4009.

malicious software. Computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

media. Defined in CNSSI 4009.

mission partner. Defined in DoDD 8000.01.

non-DoD entity. Any person who is not a civilian employee or military member of the DoD, or any entity or organization that is not a DoD Component. This includes any non-DoD federal agency and its personnel, and any contractor, grantee, awardee, partner, or party to any form of legal agreement with the DoD or another federal agency.

non-DoD information system. Any information system that is not owned, controlled, or operated by the DoD and that is not used or operated by a contractor or other non-DoD entity exclusively on behalf of the DoD. Includes information systems owned and operated by other departments and agencies of the U.S. Government; State and local governments; allies, coalition members, host nations and other nations; multinational organizations; non-governmental organizations; and the private sector.

nonpublic DoD information. Any DoD information that has not been cleared for public release in accordance with DoDD 5230.09. Nonpublic DoD information includes federal contract information that relates to a DoD contract.

on-behalf of. A situation that occurs when a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting federal information; and those activities are not incidental to providing a service or product to the government.

public DoD information. DoD information that has been cleared for public release in accordance with DoDD 5230.09.

publicly available computer. Any computer available to the general public, usually after certain conditions are met (e.g., payment of a fee, a paying guest in a hotel).

REFERENCES

Code of Federal Regulations, Title 32

Committee on National Security Systems Instruction No. 4009, "Committee on National Security Systems (CNSS) Glossary," April 6, 2015

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

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

DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2015

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

DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," March 17, 2016, as amended

DoD Instruction 4000.19, "Support Agreements," April 25, 2013, as amended

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

DoD Instruction 5230.24, "Distribution Statements on Technical Documents," August 23, 2012, as amended

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

DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 13, 2014, as amended

DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012

Federal Acquisition Regulation 52.204-21, "Basic Safeguarding of Covered Contractor Information Systems," current edition

Federal Information Processing Standards Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004

National Institute of Standards and Technology Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," December 2016, as amended

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