Department of Defense
INSTRUCTION

NUMBER 5200.01
April 21, 2016
Incorporating Change 1, Effective May 1, 2018

USD(I)

SUBJECT: DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5143.01 (Reference (a)), this instruction:

a. Reissues DoD Instruction (DoDI) 5200.01 (Reference (b)) to update policy and responsibilities for collateral, special access program, SCI, and controlled unclassified information (CUI) within an overarching DoD Information Security Program pursuant to Executive Order 13526; part 2001 of Title 32, Code of Federal Regulations; section 3038(a) of Title 50, United States Code; DoDD 5205.07; and Executive Order 13556 (References (c) through (g), respectively).

b. Establishes policy and assigns responsibilities regarding the protection, use, and dissemination of SCI within the DoD pursuant to References (a), (c), and (e) and Executive Order 12333 (Reference (h)).

2. APPLICABILITY. This instruction:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of 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 instruction as the "DoD Components").

b. Does not alter existing authorities and responsibilities of the Director of National Intelligence (DNI) or of the heads of elements of the Intelligence Community (IC) established in Reference (h) and policies issued by the DNI. Policies issued by the DNI may be obtained at https://intelshare.intelink.sgov.gov/sites/ssc/capco/policy/default.aspx.

3. POLICY. It is DoD policy that:

a. National security information will be classified, safeguarded, and declassified in accordance with References (c), (d), and DoD Manual 5200.01 (Reference (i)). CUI will be identified and safeguarded consistent with the requirements of References (g) and (i).

b. Declassification of information will receive equal attention as the classification of information so that information remains classified only as long as required by national security considerations.

c. Information will not be classified, continue to be maintained as classified, or fail to be declassified, or be designated CUI under any circumstances in order to:

(1) Conceal violations of law, inefficiency, or administrative error.

(2) Prevent embarrassment to a person, organization, or agency.

(3) Restrain competition.

(4) Prevent or delay the release of information that does not require protection in the interests of national security or as required by statute or regulation.

d. The volume of classified national security information and CUI, in whatever format or media, will be reduced to the minimum necessary to meet operational requirements.

e. The DoD Information Security Program will harmonize and align processes to the maximum extent possible to promote information sharing, facilitate judicious use of scarce resources, and simplify its management and implementation.

f. SCI will be safeguarded in accordance with policies and procedures established by the DNI.

g. Classified information released to industry will be safeguarded in accordance with DoDI 5220.22 (Reference (j)).

h. DoD Information Security Program policies, assigned responsibilities, and best practices will be developed to counter, manage, and mitigate the insider threat pursuant to DoDD 5205.16 (Reference (k)) and serious security incidents involving classified information in accordance with Reference (i) and DoDD 5210.50 (Reference (l)).

i. DoD Information Security Program policies will be developed to standardize processes and best practices in coordination with the Defense Security Enterprise pursuant to DoDD 5200.43 (Reference (m)).

j. Security requirements and responsibilities for protecting classified information and CUI from unauthorized disclosure will be emphasized in DoD Component training programs, pursuant to References (c), (d), and (i), and DoD Manual 5105.21 (Reference (n)).

k. Before being approved for public release, all DoD information will be reviewed pursuant to Reference (i); DoDD 5230.09, DoDI 5400.04, DoDI 5230.29, and DoDI 8550.01 (References (o) through (r), respectively); and other applicable policies including, but not limited to DoDD 5122.05 (Reference (s)).

l. In accordance with the provisions of section 3.7 of Reference (c), DoD will comply with guidelines set by the National Declassification Center (NDC) within the National Archives for streamlining declassification processes, facilitating quality assurance measures, and implementing standardized training regarding the declassification of records determined to have permanent historical value.

m. Safeguarding requirements and incident response measures addressing willful, negligent, and inadvertent mishandling of classified information must be implemented across DoD in accordance with Deputy Secretary of Defense Memorandum (Reference (t)). Commanders and supervisors at all levels must consider and, at their discretion, take appropriate administrative, judicial, contractual, or other corrective/disciplinary action to address negligent discharges of classified information commensurate with the seriousness of the security violation.

4. RESPONSIBILITIES. See Enclosure 2.

5. RELEASABILITY. **Cleared for public release**. ~~This instruction is available on the DoD Issuances Website at http://www.dtic.mil/whs/directives.~~ *This instruction is available on the Directives Division Website at http://www.esd.whs.mil/DD/.*

6. EFFECTIVE DATE. This instruction is effective April 21, 2016.

Marcel Lettre
Under Secretary of Defense for Intelligence

Enclosures
1. References
2. Responsibilities Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," October 24, 2014, as amended
(b) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," October 9, 2008, as amended (hereby canceled)
(c) Executive Order 13526, "Classified National Security Information," December 29, 2009
(d) Title 32, Code of Federal Regulations
(e) Section 3038(a) of Title 50, United States Code
(f) DoD Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010
(g) Executive Order 13556, "Controlled Unclassified Information," November 4, 2010.
(h) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
(i) DoD Manual 5200.01, "DoD Information Security Program," February 24, 2012
(j) DoD Instruction 5220.22, "National Industrial Security Program (NISP)," March 18, 2011
(k) DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014*, as amended*
(l) DoD Directive 5210.50, "Management of Serious Security Incidents Involving Classified Information," October 27, 2014
(m) DoD Directive 5200.43, "Management of the Defense Security Enterprise," October 1, 2012, as amended
(n) DoD Manual 5105.21, "Sensitive Compartmented Information (SCI) Administrative Security Manual," October 19, 2012
(o) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008, as amended
(p) DoD Instruction 5400.04, "Provision of Information to Congress," March 17, 2009
(q) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 13, 2014*, as amended*
(r) DoD Instruction 8550.01, "DoD Internet Services and Internet-Based Capabilities," September 11, 2012
(s) DoD Directive 5122.05, "Assistant Secretary of Defense for Public Affairs (ASD(PA))," ~~September 5, 2008~~ *August 7, 2017*
(t) Deputy Secretary of Defense Memorandum, "Unauthorized Disclosures of Classified Information or Controlled Unclassified Information on DoD Systems," August 14, 2014
(u) Executive Order 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities," August 18, 2010
(v) DoD Directive 5105.21, "Defense Intelligence Agency (DIA)," March 18, 2008
(w) DoD Instruction 3305.13, "DoD Security Education, Training, and Certification," February 13, 2014
(x) DoD 3305.13-M, "DoD Security Accreditation and Certification," March 14, 2011
(y) DoD Directive 5100.20, "National Security Agency/Central Security Service (NSA/CSS)," January 26, 2010
(z) DoD Directive 5105.60, "National Geospatial-Intelligence Agency (NGA)," July 29, 2009
(aa) DoD Directive 5105.23, "National Reconnaissance Office (NRO)," June 28, 2011, as amended

(ab) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
(ac) DoD Directive 5111.1, "Under Secretary of Defense for Policy (USD(P))," December 8, 1999
(ad) Presidential Memorandum, "Implementation of the Executive Order, 'Classified National Security Information,'" December 29, 2009
~~(ae) DoD 5200.2-R, "Personnel Security Program," January 1, 1987, as amended~~
(ae) DoD Manual 5200.02, "Procedures for the DoD Personnel Security Program (PSP)." April 3, 2017
(af) DoD Directive 5110.04, "Washington Headquarters Services (WHS)," March 27, 2013
(ag) DoD 5230.30-M, "DoD Mandatory Declassification Review (MDR) Program," December 22, 2011*, as amended*
(ah) Title 22, Code of Federal Regulations
(ai) Title 22, United States Code
(aj) Title 44, United States Code
(ak) Public Law 113-187, "Presidential and Federal Records Act Amendments of 2014," November 26, 2014
(al) Title 5, United States Code

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). As the senior security official and the senior agency official responsible for the DoD Information Security Program in accordance with References (a) and (c), the USD(I):

a. Develops, coordinates, and oversees the implementation of a DoD Information Security Program that encompasses CUI, SCI, special access programs, and collateral information and activities.

b. Develops information security policy and guidance and oversees DoD implementation of References (c) and (g), Executive Order 13549 (Reference (u)), and the DoD Information Security Program.

c. Consults, as necessary, with other Principal Staff Assistants when developing information security policy directly affecting their areas of assigned responsibilities.

d. Approves, as necessary, requests for exceptions and waivers to DoD Information Security Program policies and procedures except for those involving the responsibilities of the Under Secretary of Defense for Policy for programs listed in paragraph 7a of this enclosure and the responsibilities of the Military Departments listed in paragraph 12 of this enclosure.

e. Directs, administers, and oversees the disclosure of classified military information in category 8 (military intelligence) to foreign governments and international organizations, and coordinates with the Under Secretary of Defense for Policy on the portions of the DoD Information Security Program listed in paragraph 7a of this enclosure, including exemptions and waivers thereto.

f. In coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics and the DNI, supports research to assist the NDC in addressing the cross-agency challenges associated with declassification.

g. Coordinates with the Chief Information Officer of the Department of Defense to develop policies, including those for information assurance, that provide for the security of information in a networked environment.

2. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). Under the authority, direction, and control of the USD(I), in addition to the responsibilities in section 11 of this enclosure, and in accordance with References (a), (c), and DoDD 5105.21 (Reference (v)), the Director, Defense Intelligence Agency:

a. Maintains Reference (n).

b. Administers DoD SCI security policies and procedures issued by the DNI, except with respect to the National Security Agency/Central Security Service (NSA/CSS), National

Reconnaissance Office (NRO), and National Geospatial-Intelligence Agency (NGA). At a minimum, the Director, DIA:

(1) Incorporates within Reference (n) SCI security policies and procedures issued by the DNI, and all DNI-issued changes or modifications thereto.

(2) Inspects and accredits DoD and DoD contractor facilities for the handling, processing, storage, and discussion of SCI.

(3) Inspects accredited DoD and DoD contractor SCI facilities on a recurring basis to determine continued compliance with established SCI security policies and procedures.

(a) Issues reports detailing any deficiencies noted and corrective action required.

(b) When appropriate, shares information of mutual interest with the Directors of the Defense Security Service and Defense Contract Management Agency.

(4) As required or directed by the DNI or the USD(I), gathers data and prepares and submits reports to the DNI through the USD(I), regarding the status of implementation of SCI security policies and procedures within the DoD.

(5) Monitors the establishment and maintenance of SCI security awareness, education, and certification programs within the DoD Components in accordance with DoDI 3305.13 and DoD 3305.13-M (References (w) and (x)).

(6) Develops and coordinates recommendations on current and proposed DNI SCI security policy and procedures with the senior intelligence officials designated in accordance with References (i) and (n).

(7) On behalf of the DoD Components and their subordinate elements, establishes memorandums of agreement with NSA/CSS, NRO, and NGA and non-DoD federal agencies for joint use of SCI-accredited facilities.

(8) Operates SCI security programs to support other DoD activities and federal agencies by special agreement, in accordance with Reference (n).

3. DIRECTOR, NSA/CHIEF, CSS (DIRNSA/CHCSS). Under the authority, direction, and control of the USD(I), in addition to the responsibilities in sections 6 and 11 of this enclosure and in accordance with References (a), (c), and DoDD 5100.20 (Reference (y)), the DIRNSA/CHCSS:

a. As the designee of the Secretary of Defense, when necessary, imposes special requirements on the classification, declassification, marking, reproduction, distribution, accounting, and protection of and access to classified cryptologic information.

b. Develops implementing guidance, as necessary, for the protection of signals intelligence.

4. DIRECTOR, NGA. Under the authority, direction, and control of the USD(I), in addition to the responsibilities in sections 6 and 11 of this enclosure and in accordance with References (a), (c),

and DoDD 5105.60 (Reference (z)), the Director, NGA develops implementing guidance, as necessary, for the protection of imagery, imagery intelligence, and geospatial information.

5. DIRECTOR, NRO. Under the authority, direction, and control of the USD(I), in addition to the responsibilities in sections 6 and 11 of this enclosure and in accordance with References (a), (c), and DoDD 5105.23 (Reference (aa)), the Director, NRO develops implementing guidance, as necessary, for the protecting information related to research and development (R&D), acquisition, launch, deployment, and operation of overhead reconnaissance systems, and related data-processing facilities to collect intelligence and information to support national and DoD missions and other United States Government (USG) needs.

6. DIRNSA/CHCSS AND DIRECTORS, NRO AND NGA. Under the authority, direction and control of the USD(I), the DIRNSA/CHCSS and Directors of the NRO and NGA establish, direct, and administer all aspects of their respective organization's SCI security programs, to include all necessary coordination and implementation of DNI security policy, consistent with Reference (a) and applicable authorities as heads of elements of the IC in accordance with Reference (h).

7. UNDER SECRETARY OF DEFENSE FOR POLICY. The Under Secretary of Defense for Policy:

a. Directs, administers, and oversees those portions of the DoD Information Security Program pertaining to foreign government (including the North Atlantic Treaty Organization) classified information; the disclosure of classified military information in categories 1 through 7 to foreign governments and international organizations, consistent with DoDD 5230.11 (Reference (ab)); and security arrangements for international programs, consistent with DoDD 5111.1 (Reference (ac)) and other relevant policies.

b. Coordinates those portions of the DoD Information Security Program listed in paragraphs 1d and e of this enclosure, including exemptions and waivers thereto, with the USD(I).

c. Approves requests for exception or waiver to policy involving any policy or programs listed in paragraphs 1.d and 1.e of this enclosure.

8. UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS. In accordance with Presidential Memorandum (Reference (ad)), in coordination with the DNI and the USD(I), the Under Secretary of Defense for Acquisition, Technology, and Logistics supports research to assist the NDC in addressing the cross-agency challenges associated with declassification.

9. CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE. The Chief Information Officer of the Department of Defense coordinates with the USD(I) when developing policies, including those for information assurance, that provide for the security of information in a networked environment and are consistent with the requirements of References (i) and (n), ~~DoD 5200.2-R~~ *DoDI 5200.02* (Reference (ae)), and other guidance issued by the USD(I) and the DNI.

10. DIRECTOR, WASHINGTON HEADQUARTERS SERVICE. Under the authority, direction, and control of the ~~Department of Defense Deputy~~ Chief Management Officer *of the Department of Defense* ~~(DCMO)~~, in addition to the responsibilities in section 11 of this enclosure and in accordance with References (a), (c), and DoDD 5110.04 (Reference (af)), the Director, Washington Headquarters Service, develops implementing guidance, as necessary, for the protection of information related to providing a broad range of administrative, management, and common support services, including human resources and security clearance services, facilities and facility operations, information technology (IT) capabilities and services, financial management, acquisition and contracting, and secure communications while also providing oversight of designated DoD-wide statutory and regulatory programs, supporting DoD Components and other federal entities as directed and assigned.

a. Directs and administers a DoD Mandatory Declassification Review Program in accordance with DoD 5230.30-M (Reference (ag) and consistent with subsection 3.5 of Reference (c), to include establishing:

(1) Procedures for processing mandatory declassification review requests and appeals consistent with subsection 3.5 of Reference (c), section 2001.33 of Reference (d), and Reference (i). Procedures will ensure that requests for review of documents issued by the Inspector General of the Department of Defense are forwarded to the office of the Inspector General for processing.

(2) A database to facilitate consistency of reviews and declassification decisions.

b. Directs and administers the OSD Automatic Declassification and Review Program consistent with subsection 3.3 of Reference (c).

c. Provides for the security review of DoD information, consistent with the requirements of Reference (o), including establishing procedures for:

(1) Processing security review requests, including appeals, in accordance with References (p) and (q).

(2) Clearing of material subject to parts 120-130 of Title 22, Code of Federal Regulations and section 2751 of Title 22, United States Code (References (ah) and (ai)).

(3) Processing Department of State "Foreign Relations of the United States" documents, including appeals, consistent with Foreign Relations of the United States Program requirements (i.e., section 4353 of Reference (ai)).

11. DOD COMPONENT HEADS. The DoD Component heads:

a. Protect classified information and CUI from unauthorized disclosure consistent with References (c) and (i).

b. Designate a senior agency official to be responsible for the direction, administration, and oversight of the DoD Component's information security program, to include:

(1) Classification, declassification, and safeguarding classified information.

(2) Security education and training programs.

(3) Implementation of References (c) and (i).

c. DoD Component heads who lead IC components in accordance with Reference (h) will appoint the senior intelligence official to oversee their SCI program.

d. Ensure the senior agency official and the senior intelligence official coordinate to achieve a cohesive information security program.

e. Provide adequate funding and resources to implement classification, declassification, safeguarding, oversight, and security education and training programs.

f. Establish and maintain an ongoing self-inspection program to include periodic review and assessment of the DoD Component's classified information and CUI products.

g. Direct and administer a program for systematic declassification reviews as required by subsection 3.4 of Reference (c), to declassify records as soon as possible, but not prematurely, and for review of information subject to the automatic declassification provisions of subsection 3.3 of Reference (c).

h. Establish and maintain an active security education and training program to inform personnel of their responsibilities for protecting classified information and CUI.

(1) Train all original classification authorities and derivative classifiers in the fundamentals of security classification, the limitations of their authority, and their duties and responsibilities as a prerequisite to exercising this authority.

(2) Train all personnel to provide a basic understanding of the nature of classified information and CUI and the proper protection of such information in their possession to include responsibilities for the protection of classified information and CUI from unauthorized disclosure.

(3) Incorporate security education and training, as appropriate, into DoD contracts.

(4) Brief onsite support contractor personnel in security responsibilities, procedures, and duties applicable to their positions.

i. Submit DoD information intended for public release for review in accordance with paragraph 3.k of this Instruction.

j. Establish a system for the receipt of and action on complaints and suggestions regarding the DoD Component's information security program.

k. Forward recommendations for improvements to the DoD Information Security Program to the USD(I)'s Director for Defense Intelligence (Intelligence & Security)/Security Policy and Oversight Division.

l. Participate in the NDC by providing:

(1) The necessary resources to process declassification referrals containing DoD Component information under the purview of the NDC and in accordance with the NDC processing standards.

(2) Training to declassification reviewers in accordance with NDC training standards.

(3) Declassification reviews in accordance with the quality standards of the NDC.

(4) Initial reviews of records eligible for automatic declassification in accordance with Reference (i) and the priorities and implementing instructions issued by the NDC in accordance with References (c) and (d).

m. Ensure that classified information and CUI are managed and retained in accordance with DoD Component authorized records management manuals and schedules, as approved by the National Archives and Records Administration in accordance with Chapters 31 and 33 of Title 44, United States Code (Reference (aj)) and Public Law 113-187 (Reference (ak)).

12. SECRETARIES OF THE MILITARY DEPARTMENTS. In addition to the responsibilities in section 11 of this enclosure, the Secretaries of the Military Departments:

a. As agency heads and designated senior agency officials as defined by and in accordance with Reference (c), in cooperation with the USD(I), participate in the development and coordination of applicable Executive orders, security policy directives, and related issuances.

b. Develop and coordinate the Military Department information security policy and guidance, and oversee the Military Department implementation of References (c), (d), (i), (t) and the Military Department's Information Security Program.

c. Approve, as necessary, requests for exceptions and waivers to the Military Department's Information Security Program policies and procedures identified in paragraphs 10a and 10b of this enclosure except for those involving the responsibilities of the Under Secretary of Defense for Policy for programs listed in paragraph 7a.

13. CHAIRMAN OF THE JOINT CHIEFS OF STAFF. In addition to the responsibilities in section 11 of this enclosure, the Chairman of the Joint Chiefs of Staff provides oversight of the Combatant Commands' information security programs.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CUI	controlled unclassified information
DNI	Director of National Intelligence
DIA	Defense Intelligence Agency
DoDD	DoD Directive
DoDI	DoD Instruction
IC	Intelligence Community
NDC	National Declassification Center
NGA	National Geospatial-Intelligence Agency
NRO	National Reconnaissance Office
NSA/CSS	National Security Agency/Central Security Service
SCI	sensitive compartmented information
USD(I)	Under Secretary of Defense for Intelligence

PART II. DEFINITIONS

Unless otherwise noted, the following terms and their definitions are for the purposes of this instruction.

agency heads. "Heads of any "Executive agency," as defined in section 105 of Title 5, United States Code (Reference (al)); and "Military department," as defined in section 102 of Reference (al); and any other entity within the executive branch that comes into the possession of classified information.

collateral. All national security information classified CONFIDENTIAL, SECRET, or TOP SECRET in accordance with the provisions of an Executive order for which special systems of compartmentation (e.g., SCI or special access programs) are not formally required.

control. The authority of the agency that originates information, or its successor in function, to regulate access to the information.

CUI. A categorical designation that refers to unclassified information that does not meet the standards for national security classification pursuant to Reference (c), but requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination pursuant to and consistent with law, regulations, or Government-wide policy. The designation CUI replaces the term "sensitive but unclassified."

foreign government information. Defined in Reference (d).

IC and elements of the IC. Consistent with section 3.5(g) of Reference (h), the Office of the DNI; the Central Intelligence Agency; the NSA/CSS; the DIA; the NGA; the NRO; other offices within the DoD for the collection of specialized national foreign intelligence through reconnaissance programs; the intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps; the intelligence elements of the Federal Bureau of Investigation; the Office of National Security Intelligence of the Drug Enforcement Administration; the Office of Intelligence and Counterintelligence of the Department of Energy; the Bureau of Intelligence and Research of the Department of State; the Offices of Intelligence and Analysis of the Department of the Treasury and the Department of Homeland Security; the intelligence and counterintelligence elements of the Coast Guard; and such other elements of any department or agency as may be designated by the President, or designated jointly by the director and the head of the department or agency concerned, as an element of the IC.

information. Any knowledge that may be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the U.S. Government.

national security. Defined in Reference (c).

SAP. Defined in Reference (f).

SCI. Classified national intelligence information concerning, or derived from, intelligence sources, methods, or analytical processes that requires handling within formal access control systems established by the DNI.

senior agency official. An official appointed by a DoD Component head to direct and administer the DoD Component's information security program. The USD(I) is designated by the Secretary of Defense as the senior agency official for the DoD information security program in accordance with section 5.4(d) of Reference (c).

senior intelligence official. The highest ranking military or civilian official charged with direct foreign intelligence missions, functions, or responsibilities within a department, agency, component, or element of an IC organization.

unauthorized disclosure. A communication or physical transfer of classified information or CUI to an unauthorized recipient.