Department of Defense

INSTRUCTION

NUMBER 5200.01
October 9, 2008

USD(I)

SUBJECT: DoD Information Security Program and Protection of Sensitive Compartmented Information

References: See Enclosure 1

1. PURPOSE. This Instruction:

a. Reissues DoD Directive (DoDD) 5200.1 (Reference (a)) as a DoD Instruction (DoDI) in accordance with the guidance in DoDI 5025.01 (Reference (b)) and the authority in DoDD 5143.01 (Reference (c)).

b. Cancels DoDD 8520.1 (Reference (d)).

c. Updates policy and responsibilities for collateral, Special Access Program (SAP), and Sensitive Compartmented Information (SCI), and controlled unclassified information (CUI) within an overarching DoD Information Security Program under Reference (c) and Executive Order 12958, part 2001 of title 32, Code of Federal Regulations (CFR), section 403-5(a) of title 50, United States Code (U.S.C.), DoDD 5205.07, and Presidential Memorandum (References (e) through (i), respectively).

d. Establishes policy and assigns responsibilities regarding the protection, use, and dissemination of SCI within the Department of Defense pursuant to References (c) and (g) and Executive Order 12333 (Reference (j)).

e. Authorizes the publication of DoD 5200.1-R and DoD 5105.21-M-1 (References (k) and (l)), consistent with Reference (b).

2. APPLICABILITY AND SCOPE. 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 Department of Defense (hereafter referred to collectively 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 under Reference (j) and policies established by the DNI. Policies established by the DNI may be obtained at http://capco.dssc.sgov.gov.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. National security information shall be classified, safeguarded, and declassified in accordance with national level policy issuances. CUI shall be identified and safeguarded consistent with the requirements of References (i) and (k).

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

c. Information may not be classified or designated CUI to:

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

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

(3) Restrain competition; or

(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, shall be reduced to the minimum necessary to meet operational requirements.

e. The DoD Information Security Program, established to assure the protection of collateral, SCI, SAP, and CUI, shall 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 shall be safeguarded in accordance with policies and procedures established by the DNI.

g. Classified information released to industry shall be safeguarded in accordance with DoDD 5220.22 (Reference (m)).

h. Responsibilities for protecting classified and CUI from unauthorized disclosure shall be emphasized in DoD Component training programs, pursuant to guidelines in References (e), (f), (k), and (l).

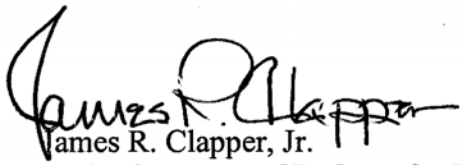
i. All DoD information approved for public release shall have been reviewed for security concerns pursuant to Reference (k); DoDDs 5230.09 and 5400.4, DoDI 5230.29, and Deputy Secretary of Defense Memorandum (References (n) through (q), respectively); and other policies as applicable.

j. Consistent with applicable laws, partnerships with appropriate DoD, government, industry, professional, academic, and international organizations should be established and fostered to gain insights to approaches, technologies, or techniques that may be of use in establishing common security practices and improving the DoD Information Security Program.

5. RESPONSIBILITIES. See Enclosure 2.

6. RELEASABILITY. This Instruction is approved for public release. Copies may be obtained through the Internet from the DoD Issuances Web Site at http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE. This Instruction is effective immediately.



James R. Clapper, Jr.
Under Secretary of Defense for Intelligence

Enclosures
1. References
2. Responsibilities

Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5200.1, "DoD Information Security Program," December 13, 1996 (hereby canceled)
(b) DoD Instruction 5025.01, "DoD Directives Program," October 28, 2007
(c) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," November 23, 2005
(d) DoD Directive 8520.1, "Protection of Sensitive Compartmented Information (SCI)," December 20, 2001 (hereby canceled)
(e) Executive Order 12958, "Classified National Security Information," April 17, 1995, as amended
(f) Part 2001 of title 32, Code of Federal Regulations (also called Information Security Oversight Office (ISOO) Directive Number 1)
(g) Section 403-5(a) of title 50, United States Code
(h) DoD Directive 5205.07, "Special Access Program (SAP) Policy," January 5, 2006
(i) Presidential Memorandum, Designation and Sharing of Controlled Unclassified Information (CUI), May 7, 2008
(j) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
(k) DoD 5200.1-R, "Information Security Program," January 14, 1997
(l) DoD 5105.21-M-1, "Department of Defense Sensitive Compartmented Information Administrative Security Manual," August 1998[1]
(m) DoD Directive 5220.22, "National Industrial Security Program," September 24, 2004
(n) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008
(o) DoD Directive 5400.4, "Provision of Information to Congress," January 30, 1978
(p) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 6, 1999
(q) Deputy Secretary of Defense Memorandum, "Web Site Administration," December 7, 1998; Attachment "Web Site Administration Policies & Procedures," November 25, 1998[2]
(r) DoD Directive 5100.20, "The National Security Agency and the Central Security Service," December 23, 1971
(s) DoD Directive 5105.60, "National Imagery and Mapping Agency (NIMA)," October 11, 1996
(t) DoD Directive 5111.1, "Under Secretary of Defense for Policy (USD(P))," December 8, 1999
(u) DoD 5200.2-R, "Personnel Security Program," January 1987
(v) Parts 120-130 of title 22, Code of Federal Regulations
(w) Sections 2751 and 4353 of title 22, United States Code

[1] Copies of this document are available at www.dia.smil.mil/admin/REG-MAN/DOD-5105.21-M-1/m1_cov.html.
[2] Copies of this document are available at www.defenselink.mil/webmasters/policy/dod_web_policy_12071998_with_amendments_and_corrections.html.

ENCLOSURE 2

RESPONSIBILITIES

l. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I) shall:

a. Serve as the Senior Security Official for the Department of Defense, consistent with Reference (c), which encompasses and addresses USD(I) responsibilities as the Senior Agency Official for the Department of Defense under subsection 5.4.(d) of Reference (e).

b. Develop, coordinate, and oversee a DoD Information Security Program (defined to include collateral, SCI, SAP, and controlled unclassified information and activities) that is effective and efficient, recognizes assigned authorities and responsibilities, and provides appropriate management safeguards to prevent fraud, waste, and abuse.

c. Oversee the implementation of security policies and procedures for collateral, SCI, SAP, and controlled unclassified information within the Department of Defense.

d. Consistent with Reference (c), represent the Secretary of Defense during the coordination of Executive orders and other policy issuances, including information security directives, policies, and procedures established for the protection of SCI by the DNI.

e. Approve, when appropriate, requests for exceptions and waivers to DoD Information Security Program policies and procedures and to the requirements of this Instruction.

f. Develop and approve DoD issuances, as necessary, to guide and direct DoD Information Security Program activities, consistent with Reference (b), consulting as appropriate with other principal staff assistants when developing information security policy directly affecting their areas of assigned responsibilities.

2. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). The Director, DIA, under the authority, direction, and control of the USD(I), shall develop Reference (l) consistent with Reference (b) and, with the exceptions of the National Security Agency/Central Security Service (NSA/CSS), National Reconnaissance Office (NRO), and National Geospatial-Intelligence Agency (NGA), administer within the Department of Defense SCI security policies and procedures issued by the DNI. As a minimum, this includes responsibility to:

a. Disseminate SCI security policies and procedures issued by the DNI, and all DNI-issued changes or modifications thereto, within the Department of Defense, in a timely and efficient manner.

b. Inspect and accredit DoD and DoD contractor facilities for the handling, processing, storage, and discussion of SCI.

c. Inspect accredited DoD and DoD contractor SCI facilities on a recurring basis to determine continued compliance with established SCI security policies and procedures and issue

reports detailing any deficiencies noted and corrective action required; when appropriate, the Director, DIA, will share information of mutual interest with the Directors of the Defense Security Service and Defense Contract Management Agency.

d. Gather data and prepare and submit such reports as may be required or directed by the DNI and/or the USD(I) regarding the status of implementation of SCI security policies and procedures within the Department of Defense. Any such reports shall be submitted to the DNI through USD(I).

e. Monitor the establishment and maintenance of SCI security awareness and education programs within the DoD Components.

f. Develop and coordinate recommendations on current and proposed DNI SCI security policy and procedures with the Senior Intelligence Officials designated according to section 10 of this enclosure.

g. On behalf of the DoD Components and their subordinate elements, establish memorandums of agreement with NSA/CSS, NRO, and NGA and non-DoD Federal agencies for joint use of SCI-accredited facilities.

h. Operate SCI security programs to support other DoD activities and Federal agencies by special agreement, as required.

3. DIRECTORS, NSA/CSS, NRO, and NGA. The Directors of the NSA/CSS, NRO, and NGA, with the oversight of the USD(I), shall 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 (c) and applicable authorities as heads of elements of the Intelligence Community under Reference (j).

4. DIRECTOR, NSA/CSS. The Director, NSA/CSS, under the authority, direction, and control of the USD(I), in addition to the responsibilities in sections 3 and 9 of this enclosure and in accordance with Reference (c), shall:

a. As the designee of the Secretary of Defense, when necessary, impose special requirements on the classification, declassification, marking, reproduction, distribution, accounting, and protection of and access to classified cryptologic information, in accordance with Reference (e) and DoDD 5100.20 (Reference (r)).

b. Develop implementing guidance, as required, for the protection of signals intelligence in accordance with Reference (r).

5. DIRECTOR, NGA. The Director, NGA, under the authority, direction, and control of the USD(I), in addition to the responsibilities in sections 3 and 9 of this enclosure and in accordance with Reference (c), shall develop implementing guidance, as required, for the protection of

imagery, imagery intelligence, and geospatial information in accordance with DoDD 5105.60 (Reference (s)).

6. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). The USD(P) shall:

a. Direct, administer, and oversee those portions of the DoD Information Security Program pertaining to foreign government (including the North Atlantic Treaty Organization) classified information, the National Disclosure Policy, and security arrangements for international programs, consistent with DoDD 5111.1 (Reference (t)) and other appropriate policies.

b. Coordinate those portions of the DoD Information Security Program listed in paragraph 6.a., including exemptions and waivers thereto, with the USD(I).

c. Approve requests for exception or waiver to policy involving any programs listed in paragraph 6.a., when appropriate.

7. ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DoD CHIEF INFORMATION OFFICER (ASD(NII)/DoD CIO). The ASD(NII)/DoD CIO shall coordinate with the USD(I) when developing policies, including those for information assurance, which provide for the security of information in a networked environment and are consistent with, as appropriate, the requirements of References (k) and (l), DoD 5200.2-R (Reference (u)), and other guidance issued by the USD(I) and the DNI.

8. DIRECTOR, WASHINGTON HEADQUARTERS SERVICE (WHS). The Director, WHS, under the authority, direction, and control of the Director of Administration and Management, shall:

a. Direct and administer a DoD Mandatory Declassification Review Program consistent with subsection 3.5 of Reference (e).

(1) Establish procedures for processing mandatory declassification review requests, including appeals, consistent with subsection 3.5(d) of Reference (e), section 2001.33 of Reference (f), and Reference (k). Procedures shall ensure that requests for review of documents issued by the Inspector General of the Department of Defense are forwarded to that office for processing.

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

b. Direct and administer the OSD Automatic Declassification and Review Program consistent with subsection 3.3 of Reference (e).

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

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

(2) Clearance of material subject to parts 120-130 of title 22, CFR and section 2751 of title 22, U.S.C. (References (v) and (w)).

(3) Processing Department of State Foreign Relations of the U.S. (FRUS) documents, including appeals, consistent with FRUS Program requirements (section 4353 of Reference (w)).

9. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

a. Protect classified and controlled unclassified information from unauthorized disclosure consistent with References (e) and (k), as appropriate.

b. Designate a Senior Agency Official for their respective Component who shall be responsible for the direction, administration, and oversight of the Component's information security program, to include classification, declassification, safeguarding, oversight, and security education and training programs, and for the efficient and effective implementation of References (e) and (k).

c. Ensure the Component Senior Agency Official and the Component Senior Intelligence Official coordinate as appropriate to achieve a harmonized and cohesive information security program within the DoD Component.

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

e. Establish and maintain an ongoing self-inspection program to include periodic review and assessment of the Component's classified and controlled unclassified information products.

f. Direct and administer a program for systematic declassification reviews as required by subsection 3.4 of Reference (e), 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 (e).

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

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

(2) All personnel shall receive training that provides a basic understanding of the nature of classified and controlled unclassified information and the proper protection of such information in their possession.

(3) The requirement for security education and training shall be incorporated, as appropriate, into DoD contracts.

(4) Onsite support contractor personnel shall receive briefings in security responsibilities, procedures, and duties applicable to their positions.

h. Submit DoD information intended for public release for review in accordance with References (n), (p), and (q), and other applicable DoD policy.

i. Establish a system to consider and take action on complaints and suggestions regarding the Component's information security program.

j. Forward recommendations for improvements to the DoD Information Security Program to the Director of Security, Office of the Deputy Under Secretary of Defense for HUMINT, Counterintelligence & Security (DUSD(HCI&S)).

10. HEADS OF THE DoD COMPONENTS THAT ARE NOT ELEMENTS OF THE INTELLIGENCE COMMUNITY. The Heads of the DoD Components that are not elements of the Intelligence Community, as specified by Reference (j), shall designate, at an appropriate level, a Senior Intelligence Official who shall be responsible for the effective implementation of SCI security policies and security awareness and education programs within the Component, consistent with Reference (l). This designation shall be reported to the USD(I).

11. SECRETARIES OF THE MILITARY DEPARTMENTS. The Secretaries of the Military Departments, in addition to the responsibilities in section 9 of this enclosure, as Agency Heads under Reference (e) shall, in cooperation with the USD(I), participate in the development and coordination of applicable Executive orders, security policy directives, and related issuances.

12. DoD SENIOR INTELLIGENCE OFFICIALS. DoD Senior Intelligence Officials, including those who are heads of elements of the Intelligence Community and those designated according to section 10 of this enclosure, shall:

a. Protect intelligence and intelligence sources and methods from unauthorized disclosure consistent with the policies of the DNI and, where applicable, the requirements of References (k) and (l). Administer and oversee, within their respective organizations, those aspects of the SCI security programs not delegated to DIA in section 2 of this enclosure.

b. Provide adequate funding and other resources for effective implementation of SCI security policies and procedures and associated security awareness and education programs within the DoD Component.

c. Ensure that applicable security policies and procedures issued by the DNI and the USD(I), including all changes or modifications thereto, are implemented within the DoD Component.

d. Participate as appropriate in the DNI's processes for the development and coordination of SCI security policy and procedures.

e. When required, develop and publish DoD Component-specific implementation guidance, policies, or regulations for the protection of SCI information and programs.

f. Provide to the DUSD(HCI&S) copies of requests for exceptions and waivers to information security policies issued by the DNI concurrent with submission to DNI for approval. Requests from Senior Intelligence Officials designated according to section 10 of this enclosure shall be submitted to the DNI through DIA.

g. Employ risk management processes to minimize the potential for compromise of intelligence and intelligence sources and methods, while maximizing the sharing of information.

13. CHAIRMAN OF THE JOINT CHIEFS OF STAFF. The Chairman of the Joint Chiefs of Staff, in addition to the responsibilities in section 9 of this enclosure, shall provide oversight of the Combatant Commands' information security programs.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
CFR	Code of Federal Regulations
CUI	controlled unclassified information
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
DUSD(HCI&S)	Deputy Under Secretary of Defense for HUMINT, Counterintelligence & Security
FRUS	Foreign Relations of the United States
HUMINT	human intelligence
NGA	National Geospatial Intelligence Agency
NRO	National Reconnaissance Organization
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
OSD	Office of the Secretary of Defense
SAP	Special Access Program
SBU	sensitive but unclassified
SCI	Sensitive Compartmented Information
USC	United States Code
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
WHS	Washington Headquarters Service

PART II. DEFINITIONS

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

collateral. All national security information classified Confidential, Secret, or Top Secret under the provisions of an Executive order for which special systems of compartmentation (such as SCI or SAPs) 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 under Reference (e), but is pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. The designation CUI replaces the term "sensitive but unclassified" (SBU).

DoD SAP. Defined in Reference (h).

foreign government information. Defined in Reference (e).

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.

Intelligence Community and elements of the Intelligence Community. Consistent with section 3.5(h) of Reference (j), the Office of the DNI; the Central Intelligence Agency; the NSA; the DIA; the NGA; the NRO; other offices within the Department of Defense 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 Intelligence Community.

national security. Defined in Reference (e).

Senior Agency Official. An official appointed by the Head of a DoD Component to direct and administer the Component's information security program.

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 Intelligence Community organization.

SCI. Classified national intelligence information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the DNI.

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