



Department of Defense INSTRUCTION

NUMBER 8523.01
April 22, 2008

ASD(NII)/DoD CIO

SUBJECT: Communications Security (COMSEC)

- References:
- (a) DoD Directive C-5200.5, "Communications Security (COMSEC) (U)," April 21, 1990 (hereby canceled)
 - (b) DoD Instruction 5025.01, "DoD Directives Program," October 28, 2007
 - (c) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
 - (d) Committee on National Security Systems Policy (CNSSP) No. 1, "National Policy for Safeguarding and Control of COMSEC Materials," September 2004¹
 - (e) through (p), see Enclosure 1

1. PURPOSE

This Instruction:

- 1.1. Reissues and renumbers Reference (a) as a DoD Instruction in accordance with the guidance in Reference (b) and the authority in Reference (c).
- 1.2. Establishes and implements DoD COMSEC policy in accordance with Reference (d) and DoD Directive (DoDD) 8500.01E (Reference (e)).
- 1.3. Supersedes DoD Instructions 4660.2, 5210.74, and S-5225.1 (References (f), (g), and (h)).
- 1.4. Authorizes the publication of implementing procedures for COMSEC.

2. APPLICABILITY AND SCOPE

This Instruction:

¹ Available at <http://www.cnss.gov>

2.1. 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 in the Department of Defense (hereafter referred to collectively as the “DoD Components”).

2.2. Applies to DoD-owned information systems (ISs) and DoD-controlled ISs operated by a contractor or other entity on behalf of the Department of Defense that receive, process, store, display, or transmit DoD information, regardless of classification or sensitivity, consistent with Reference (e).

2.3. Does not alter or supersede the existing authorities and policies of the Director of National Intelligence regarding the protection of sensitive compartmented information and special access programs for intelligence as directed by Executive Order 12333 (Reference (i)) and other laws and regulations.

3. DEFINITIONS

Terms used in this Instruction are defined in Enclosure 2 of Reference (e), Joint Publication 1-02 (Reference (j)), and CNSS Instruction (CNSSI) No. 4009 (Reference (k)).

4. POLICY

The ability to maintain the confidentiality, integrity, and availability of DoD classified information and unclassified information that has not been approved for public release during transmission is of paramount importance for an effective DoD security posture. Therefore, it is DoD policy that:

4.1. Transmission of DoD information shall be protected through the COMSEC measures and procedures set forth in this Instruction and its implementing procedures.

4.2. COMSEC materials shall be developed, acquired, operated, maintained, and disposed of through the approved methods set forth in this Instruction and its implementing procedures.

4.3. A program to ensure operational availability of commonly used COMSEC equipment during crisis or contingencies shall be established and maintained.

4.4. COMSEC equipment shall be compatible with DoD-approved key management systems.

4.5. Controlled cryptographic items (CCI) shall be accounted for in the COMSEC Material Control System (CMCS) (Reference (d)), an equivalent material control system, or a combination of the two that provides accountability and visibility of the CCI. Any system

chosen must meet the provisions of Annex C of National Security Telecommunications and Information Systems Security Instruction No. 4001 (Reference (I)).

4.6. Classified cryptographic devices and unencrypted keying material shall be accounted for in the CMCS. Encrypted keying material may be handled and tracked similarly if desired.

4.7. COMSEC equipment users and maintenance technicians shall be appropriately trained, to include certification if required.

4.8. The Department of Defense shall follow Committee on National Security Systems (CNSS) COMSEC policy documents as issued. These are available on the NIPRNET at <http://www.cnss.gov> or on the SIPRNET at http://www.iad.nsa.smil.mil/resources/library/cnss_section/index.cfm.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) shall:

5.1.1. Oversee implementation of this Instruction and develop additional DoD COMSEC policy as required.

5.1.2. Ensure DoD COMSEC activities:

5.1.2.1. Comply with applicable national policies and guidance.

5.1.2.2. Are compatible with planned and existing DoD information systems.

5.1.2.3. Meet objectives for commonality, interoperability, compatibility, standardization, and survivability.

5.1.3. Confirm requirements for COMSEC research and development (R&D) and for COMSEC product and system acquisition in concert with emergent DoD Component needs. Forward confirmed requirements to the Director, National Security Agency (DIRNSA).

5.1.4. Review proposed COMSEC programs and the resource requirements and recommend resource allocations.

5.2. The Chairman of the Joint Chiefs of Staff shall:

5.2.1. Review and validate all joint requirements for COMSEC and forward validated COMSEC requirements to the DIRNSA.

5.2.2. Review planned and existing COMSEC solutions in relation to joint interoperability, plans, and objectives.

5.2.3. Validate requirements for the COMSEC Utility Program (CUP) assets in accordance with CNSSI No. 4007 (Reference (m)).

5.2.4. Validate combatant command interoperability requirements to release COMSEC products or associated COMSEC information to any foreign government in accordance with Chairman of the Joint Chiefs of Staff Instruction 6510.06A (Reference (n)).

5.3. The Director, Defense Information Systems Agency, under the authority, direction, and control of the ASD(NII)/DoD CIO, shall ensure that the Joint Interoperability Test Center tests and certifies COMSEC interoperability, as required.

5.4. The Director, Defense Security Service, under the authority, direction, and control of the Under Secretary of Defense for Intelligence (USD(I)), shall:

5.4.1. Monitor COMSEC practices of DoD contractors in accordance with DoDD 5220.22 (Reference (o)).

5.4.2. Inspect COMSEC accounts as a portion of regular industrial security inspections at DoD contractor facilities in coordination with the applicable central office of record (COR).

5.5. The DIRNSA, under the authority, direction, and control of USD(I), as the DoD COMSEC Program Manager and, consistent with the National Manager responsibilities assigned to DIRNSA by National Security Directive 42 (Reference (p)), shall:

5.5.1. Serve as the DoD COMSEC and cryptography focal point and manage the implementation of this Instruction.

5.5.2. Serve as the centralized COMSEC acquisition authority.

5.5.3. In coordination with the Heads of the DoD Components, implement established policies and develop plans, procedures, training, and mechanisms for DoD Components, contractors, and subcontractors.

5.5.4. In coordination with DoD Components, establish standards for and conduct evaluations of COMSEC products and services and endorse these standards for use by DoD Components, contractors, and subcontractors.

5.5.5. Conduct, approve, or endorse R&D of COMSEC products and services needed to fulfill validated requirements for COMSEC and to advance technology. Delegate authority to conduct specified cryptographic R&D to DoD Components, when mutually agreed.

5.5.6. Prescribe the standards, methods, and procedures for operation, management, and protection of COMSEC material.

5.5.7. Conduct COMSEC liaison with foreign governments and with international organizations, as dictated by operational requirements.

5.5.8. Facilitate the exchange of COMSEC information among DoD Components, the North Atlantic Treaty Organization, and other allies and/or coalition partners.

5.5.9. Operate printing and fabrication facilities as required to perform critical functions related to the provision of COMSEC material.

5.5.10. Administer the CUP, a rotating pool of COMSEC equipment, which shall be sold or loaned to users having an urgent requirement for COMSEC protection that was not budgeted or programmed per Reference (m).

5.5.11. Prescribe security standards for the performance of COMSEC COR responsibilities by DoD Components. Maintain a National Office of Record to oversee DoD Component CORs.

5.6. The Heads of DoD Components shall:

5.6.1. Implement all applicable COMSEC policies, directives, criteria, standards, and doctrine within their respective DoD Components.

5.6.2. Review and validate all DoD Component requirements for COMSEC products and services and forward validated COMSEC requirements to the DIRNSA as necessary to support procurement activities.

5.6.3. Plan, program, fund, implement, manage, and provide logistics support to the COMSEC aspects of their information systems. This shall include centralized record maintenance of COMSEC material at the DoD Component level.

5.6.4. Manage the DoD Component responsibilities of the CMCS. Perform the functions of the Service Authority.

5.6.5. Establish and maintain a DoD Component-wide COMSEC assessment program to evaluate compliance with DoD, Joint Staff, and DoD Component policy and procedures. Assessment will include management effectiveness of COMSEC incident reporting, oversight of CCI accountability, currency and accuracy of the cryptographic access program, application of standardized COMSEC training, and general CMCS compliance.

5.6.6. Develop, maintain, and modify DoD Component-level policies, procedures, training programs, and software systems that ensure uniform application of the policies contained herein.

6. PROCEDURES

6.1. Only National Security Agency/Central Security Service (NSA/CSS)-approved COMSEC products and services shall be used to secure classified information.

6.2. Sensitive information as defined in Reference (e) and information that has not been approved for public release processed on DoD information systems shall be protected by products validated by the National Institute of Standards and Technology as meeting the criteria of applicable Federal Information Processing Standards, or by NSA/CSS-approved COMSEC products and services.

6.3. DoD Components shall acquire COMSEC products and services through the NSA/CSS that serves as the centralized COMSEC acquisition authority. If the products and services are unavailable through centralized procurement, the DoD Components shall acquire them directly from commercial entities that are authorized by the NSA/CSS to sell such products and services.

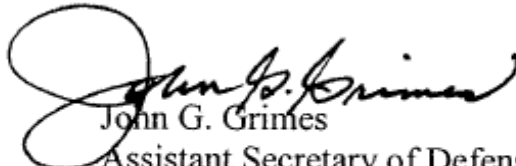
6.4. Validated COMSEC requirements for all DoD information systems, including those integral to weapons systems and weapons support systems, shall be addressed throughout the system life cycle (e.g., concept definition, design and development, test and evaluation, procurement, installation, operation, maintenance, and disposal).

7. RELEASABILITY

UNLIMITED. 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>.

8. EFFECTIVE DATE

This Instruction is effective immediately.


John G. Grimes
Assistant Secretary of Defense for
Networks and Information Integration/
DoD Chief Information Officer

Enclosures – 2

- E1. References, continued
- E2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

- (e) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
- (f) DoD Instruction 4660.2, "Communications Security (COMSEC) Equipment Maintenance and Maintenance Training," June 3, 1992 (hereby canceled)
- (g) DoD Instruction 5210.74, "Security of Defense Contractor Telecommunications," June 26, 1985 (hereby canceled)
- (h) DoD Instruction S-5225.1, "Communications Security (COMSEC) Assistance to Foreign Governments and International Organizations (U)," November 4, 1983 (hereby canceled)
- (i) Executive Order 12333, "United States Intelligence Activities," December 4, 1981; as amended by EO 13284, January 23, 2003, and EO 13355, August 27, 2004
- (j) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," as amended
- (k) Committee on National Security Systems Instruction No. 4009, "National Information Assurance (IA) Glossary," as revised June 2006²
- (l) National Security Telecommunications and Information Systems Security Instruction No. 4001, "(U) Controlled Cryptographic Items," July 1996³
- (m) Committee on National Security Systems Instruction No. 4007, "Communications Security (COMSEC) Utility Program," November 2007²
- (n) Chairman of the Joint Chiefs of Staff Instruction 6510.06A, "Communications Security Releases to Foreign Nations," December 18, 2006
- (o) DoD Directive 5220.22, "National Industrial Security Program," September 27, 2004
- (p) National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990⁴

² Available at <http://www.cnss.gov>

³ Available on the SIPRNET at http://www.iad.nsa.smil.mil/resources/library/cnss_section/cnss_instructions.cfm

⁴ Available on the SIPRNET at <http://www.iad.nsa.smil.mil/resources/library>

E2. ENCLOSURE 2

DEFINITIONS

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

E2.1. Central Office of Record. See CNSSI No. 4009 (Reference (k)).

E2.2. COMSEC. See Reference (k).

E2.3. COMSEC Material. See Reference (k).

E2.4. COMSEC Material Control System. See Reference (k).

E2.5. Controlled Cryptographic Item. See Reference (k).

E2.6. Information System. See Reference (i).

E2.7. National Office of Record. The body within the National Security Agency that provides central offices of record (CORs) with national-level guidance, assistance, and oversight and ensures that CORs adhere to published standards, methods, and procedures for protecting cryptographic material.

E2.8. National Security Agency/Central Security Service (NSA/CSS)-Approved. NSA/CSS approval may consist of: (1) product certification wherein NSA/CSS or its designee evaluates a product and certifies that it meets defined criteria, allowing certain defined usage; or (2) product or system approval wherein NSA/CSS approves a set of generic solutions. In the latter case, the approved solution may consist of a combination of components. The use of this combination of components allows a user to protect information of the type specified in the NSA/CSS approval specification.

E2.9. Sensitive Information. See Reference (e).

E2.10. Service Authority. DoD Component-level organization that performs COMSEC activity functions in support of the COR. Service Authority activities include oversight for COMSEC operations, policy, procedures, and training. Service Authority roles may include cryptographic hardware management and distribution control; approving account establishment; approving authority for certification approval authorities; implementing COMSEC Material Control System/Key Management Infrastructure policy and procedures; direct operational support; final adjudication authority within each Service for determining when reported COMSEC incidents result in COMSEC insecurities; management and oversight of formal account inspection or audit program; registration authority for public key infrastructure local registration authorities; and ensuring Service compliance with COMSEC access program requirements.