DoD Instruction 8523.01

Communications Security

Originating Component:	Office of the DoD Chief Information Officer
Effective:	January 6, 2021
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction 8523.01, "Communications Security (COMSEC)," April 22, 2008
Approved by:	Dana Deasy, DoD Chief Information Officer

Purpose: In accordance with the authority in DoD Directive 5144.02, DoD Instruction 8500.01, and the Committee on National Security Systems Policy (CNSSP) No. 1, this issuance establishes policy, assigns responsibilities, and provides procedures for managing communications security (COMSEC).

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

1.2. POLICY.

It is DoD policy to:

a. Protect the communication of DoD information through the use of COMSEC measures, including the use of transmission security (TRANSEC), to safeguard communications. This includes protecting wired, wireless, and space systems from detection, traffic analysis, traffic flow security, intercept, jamming, and exploitation.

b. Maintain an inventory of COMSEC equipment, including controlled cryptographic items (CCI) and cryptographic high value products, and material that protects the confidentiality, integrity, and availability of classified and controlled unclassified information throughout the intelligence life of the information while withstanding attacks from emerging threats.

c. Plan for, program, budget, and integrate modernized cryptographic solutions before decertification of cryptographic products, protocols, and algorithms.

SECTION 2: RESPONSIBILITIES

2.1. DOD CHIEF INFORMATION OFFICER (DOD CIO).

The DoD CIO:

a. Oversees the implementation of this issuance and develops additional COMSEC policy as required.

b. Implements policies and procedures to ensure the development of plans and programs to secure national security systems (NSS) against technical exploitation threats, including the development of necessary security architectures.

c. Approves and provides minimum security standards and policy for NSS.

d. Ensures COMSEC activities:

(1) Comply with applicable national policies and guidance.

(2) Are compatible with planned and existing DoD information systems.

(3) Meet objectives for confidentiality, integrity, commonality, interoperability, compatibility, standardization, availability, and survivability.

e. Identifies and prioritizes requirements for COMSEC research and development (R&D) and COMSEC product and system acquisition in conjunction with emergent DoD Component needs. Forwards confirmed requirements to the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS).

f. Reviews and assesses National Security Agency/Central Security Service (NSA/CSS) recommendations on proposed DoD Component national security telecommunications and information systems security programs and budgets.

g. Monitors and reviews the overall COMSEC, cryptographic modernization, and key management programs of the DoD pursuant to Section 189 of Title 10, United Stated Code.

h. Establishes and chairs the COMSEC Review and Advisory Board pursuant to Section 189 of Title 10, United States Code.

2.2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY.

Under the authority direction, and control of the DoD CIO and in addition to the responsibilities in Paragraph 2.5., the Director, Defense Information Systems Agency ensures the Joint Interoperability Test Command tests and certifies COMSEC interoperability, as required.

2.3. DIRECTOR, DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY.

Under the authority, direction, and control of the Under Secretary of Defense for Intelligence and Security and in addition to the responsibilities in Paragraph 2.5., the Director, Defense Counterintelligence and Security Agency:

a. Monitors COMSEC practices of DoD contractors in accordance with DoDD 5105.42 and DoDI 5220.22.

b. In coordination with the NSA/CSS central office of record (COR), includes COMSEC accounts during industrial security reviews at DoD contractor facilities in accordance with NSA/CSS Policy Manual 3-16 at https://www.iad.nsa.smil.mil/resources/library/index.cfm.

2.4. DIRNSA/CHCSS.

Under the authority, direction, and control of the Under Secretary of Defense for Intelligence and Security and in addition to the responsibilities in Paragraph 2.5., the DIRNSA/CHCSS:

a. Serves as the COMSEC Program Manager, in accordance with the National Manager responsibilities in DoDD 5100.20.

b. Serves as the COMSEC and cryptography focal point, including the transformation, modernization, and replacement of cryptographic solutions, and manages the implementation of this issuance.

c. Serves as the centralized COMSEC acquisition authority.

d. Implements established policies and develops plans, procedures, training, and mechanisms for DoD Components, contractors, and subcontractors in coordination with the DoD Component heads.

e. Establishes standards and conducts evaluations of COMSEC products, solutions, and services. Evaluates and approves deviations from NSA/CSS established standards.

f. Conducts, approves, or endorses R&D of COMSEC products and services needed to fulfill validated requirements for COMSEC and to advance technology.

g. Delegates authority to conduct specified cryptographic R&D to DoD Components, when mutually agreed.

h. Assigns standards, methods, and procedures for the operation, management, and protection of COMSEC material.

i. Conducts COMSEC liaison with foreign governments and with international organizations.

j. Facilitates the exchange of COMSEC information among DoD Components, the North Atlantic Treaty Organization, and other allies and coalition partners.

k. Operates printing, fabrication, and electronic key management facilities as required to perform critical functions related to the provision of COMSEC material.

l. Administers the COMSEC Utility Program (CUP) in accordance with Committee on National Security Systems Instruction (CNSSI) No. 4007.

m. Establishes COR responsibilities and maintains a National Office of Record to oversee all CORs.

n. Audits COMSEC accounts falling under the jurisdiction of the NSA/CSS COR.

o. Develops policies or guidance for using or interconnecting COMSEC products, services, and solutions of foreign origin and distributing NSA/CSS-approved cryptographic equipment to foreign governments and international organizations in accordance with NSA/CSS policy or guidance.

p. Develops policies, guidance, criteria and associated threat and risk assessments for authorizing integration, installation, and use of NSA/CSS-certified COMSEC products and information by foreign integrators, installers, or vendors.

q. Assesses the overall security posture of, and disseminates information on, threats to, and vulnerabilities of NSS.

r. Requests from the DoD Component heads information and technical support needed to execute assigned responsibilities.

s. Reviews and assesses DoD Component national security telecommunications systems security programs and budgets annually and recommend alternatives, where appropriate, on behalf of the DoD CIO.

t. Reviews and approves all COMSEC, cybersecurity and, in conjunction with other DoD Components, TRANSEC standards, techniques, systems, and equipment for applications within NSS.

2.5. DOD COMPONENT HEADS.

The DoD Component heads:

a. Achieve and maintain secure NSS within their respective Components.

b. Implement applicable COMSEC policies, directives, criteria, standards, and doctrine within their respective Components.

c. Review and validate their respective requirements for COMSEC products and services, and forward validated COMSEC requirements to the DIRNSA/CHCSS, as necessary, to support procurement activities.

d. Plan, program, fund, implement, manage, and provide logistics support to the COMSEC aspects of their information systems, including centralized record maintenance of COMSEC material at the DoD Component level, and ensure replacement COMSEC is fielded before decertification.

e. Manage their responsibilities of the COMSEC Material Control System (CMCS) and perform the functions of the Service Authority.

f. Establish and maintain a DoD Component-wide COMSEC assessment program to evaluate compliance with DoD, Joint Staff, and DoD Component policy and procedures. The assessment will include:

(1) Management effectiveness of COMSEC incident reporting.

(2) Oversight of COMSEC accountability, currency, and accuracy of the cryptographic access program.

(3) Application of standardized COMSEC training.

(4) General CMCS compliance (e.g., CMCS for CCI).

g. Develop, maintain, and modify DoD Component-level policies, procedures, training programs, and software systems that ensure uniform application of this issuance.

h. As directed by the DoD CIO, report the status and compliance of COMSEC-related matters to include cryptographic and COMSEC modernization, key management, and other issues or topics required by the DoD CIO.

i. Develop, acquire, operate, maintain, and dispose of COMSEC materials in accordance with this issuance.

j. Ensure COMSEC equipment is compatible with DoD-approved key management systems.

k. Account for COMSEC material in accordance with CNSSIs No. 4001 and 4005.

l. Account for cryptographic high value products in accordance with CNSSI No. 4031.

m. Train COMSEC equipment users and maintenance technicians to include certification in accordance with CNSSI No. 4001.

n. Implement processes and procedures for the routine destruction and emergency protection of COMSEC material countermeasures in accordance with CNSSI No. 4004.1.

o. Implement emissions security and transient electromagnetic pulse surveillance technology countermeasures in accordance with CNSSP No. 300 and CNSSI No. 7000.

p. Implement COMSEC requirements for space systems countermeasures in accordance with CNSSP No. 12.

q. Use COMSEC products, services, and solutions of foreign origin and distribute NSA/CSS-approved cryptographic equipment to foreign governments and international organizations only in accordance with NSA/CSS policy and guidance.

r. Integrate, install, or use of NSA/CSS-certified COMSEC products and information using foreign integrators and installers on any weapon platform or system countermeasures in accordance with NSA/CSS policy, guidance, assessment, and criteria.

s. Ensure all cryptographic development programs and products sponsored or endorsed by their respective components, and developed under the Commercial COMSEC Evaluation Program, vendor partnerships, User Partnership Program, and any similar program must meet the requirements in NSA/CSS Policy 3-9.

t. Use NSA/CSS-approved COMSEC, to include TRANSEC, measures for the protection of classified information or products validated by the National Institute of Standards and Technology for protection of controlled unclassified information.

u. Submit cryptographic key extension requests in accordance with Chairman of the Joint Chiefs of Staff Instruction 6510.02E.

2.6. CHAIRMAN OF THE JOINT CHIEFS OF STAFF.

The Chairman of the Joint Chiefs of Staff:

a. Reviews and validates all joint requirements for COMSEC and forwards validated COMSEC requirements to the DIRNSA/CHCSS.

b. Reviews planned and existing COMSEC solutions in relation to joint interoperability, plans, and objectives.

c. Validates requirements for CUP assets in accordance with CNSSI No. 4007.

d. Validates 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 6510.06C and CNSSP No. 8.

e. Issues cryptographic modernization planning instructions to DoD Components.

SECTION 3: PROCEDURES

3.1. PRODUCTS AND SERVICES.

a. DoD Components must use NSA/CSS-approved COMSEC products and services to secure the communication and protect classified transmission-related information of NSS.

b. DoD Components must use NSA/CSS-approved or National Institute of Standards and Technology-certified products and services to secure the communications and protect transmission-related information of systems not identified as NSS.

3.2. COMSEC PRODUCT ACQUISITION AND REQUIREMENTS.

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

b. DoD Components must address validated COMSEC requirements for all DoD information systems, including those integral to weapons systems and weapons support systems, throughout the system life cycle (i.e., concept definition, design and development, test and evaluation, procurement, installation, operation, maintenance, and disposal).

c. If DoD Components determine that TRANSEC measures are required, they will acquire TRANSEC products and services to address current and future threats to communication transmissions in accordance with NSA/CSS TRANSEC procedures and guidance.

d. DoD Components will use, where appropriate, streamlined, rapid, and iterative approaches from development to fielding to increase delivery speed of encryption and TRANSEC equipment and products.

(1) Prototyping and experimentation will be used before defining their requirements and determining commercial off-the-shelf systems.

(2) Platform electronics and software must be designed for routine update or replacement instead of static configurations that last more than a decade.

e. The DoD Components will ensure the product meets/achieves NSA/CSS approval/certification for NSS and NSA/CSS approval or National Institute of Standards and Technology certification to the appropriate level for non-NSS products.

f. Products used to protect NSS or classified information that also require cryptographic products or services must use NSA/CSS-approved public key and key management infrastructures. These products and services must be addressed throughout the life cycle of their program.

g. The vendor or developer and supporting NSA/CSS Cybersecurity Certification Manager must use NSA/CSS requirements to complete and submit those technical reports required for NSA/CSS certification or approval.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
CCI	controlled cryptographic item
CMCS	Communications Security Material Control System
CNSSI	Committee on National Security Systems instruction
CNSSP	Committee on National Security Systems policy
COMSEC	communications security
COR	central office of record
CUP	Communications Security Utility Program
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DoD CIO	DoD Chief Information Officer
NSA/CSS	National Security Agency/Central Security Service
NSS	national security systems
R&D	research and development
TRANSEC	transmission security

G.2. DEFINITIONS.

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

TERM	DEFINITION
CCI	Defined in CNSSI No. 4009.
COMSEC	Defined in CNSSI No. 4009.
COMSEC equipment	Defined in CNSSI No. 4009.
controlled unclassified information	Defined in CNSSI No. 4009.
CUP	A rotating pool of COMSEC equipment, which must be sold or loaned to users having an urgent requirement for COMSEC protection that was not budgeted or programmed.
emissions security	Defined in CNSSI No. 4009.

TERM	DEFINITION
intelligence life	The amount of time in years that information must be protected.
service authority	Defined in CNSSI No. 4005.
transient electromagnetic pulse surveillance technology	Defined in CNSSI No. 4009.
traffic flow security	Defined in CNSSI No. 4009.
TRANSEC	Defined in CNSSI No. 4009.

REFERENCES

Chairman of the Joint Chiefs of Staff Instruction 6510.02E, "Cryptographic Modernization Planning," April 1, 2014

Chairman of the Joint Chiefs of Staff Instruction 6510.06C, "Communications Security Releases to Foreign Nations," November 8, 2013

Committee on National Security Systems Instruction No. 4001, "Controlled Cryptographic Items," May 7, 2013

Committee on National Security Systems Instruction No. 4004.1, "Destruction and Emergency Protection Procedures for COMSEC and Classified Material," August 2006, as amended

Committee on National Security Systems Instruction No. 4005, "Safeguarding Communications Security (COMSEC) Facilities and Materials," August 22, 2011

Committee on National Security Systems Instruction No. 4007, "Communications Security (COMSEC) Utility Program," November 1, 2007

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

Committee on National Security Systems Instruction No. 4031, "Cryptographic High Value Products," September 18, 2019

Committee on National Security Systems Instruction No. 7000, "TEMPEST Countermeasures for Facilities," May 2004

Committee on National Security Systems Policy No. 1, "National Policy for Safeguarding and Control of COMSEC Materials," September, 2004

Committee on National Security Systems Policy No. 8, "Policy Governing the Release and Transfer of U.S. Government Cryptologic National Security Systems Technical Security Material, Information, and Techniques to Foreign Governments and International Organizations," August 1, 2012

Committee on National Security Systems Policy No. 12, "Cybersecurity Policy for Space Systems Used to Support National Security Missions," February, 2018

Committee on National Security Systems Policy No. 300, "National Policy on Control of Compromising Emanations," April 2004

DoD Directive 5100.20, "National Security Agency/Central Security Service (NSA/CSS)," January 26, 2010

DoD Directive 5105.42, "Defense Security Service (DSS)," August 3, 2010, as amended

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

DoD Instruction 5220.22, "National Industrial Security Program (NISP)," March 18, 2011, as amended

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

National Security Agency/Central Security Service Policy 3-9, "Cryptographic Modernization," April 12, 2018

National Security Agency/Central Security Service Policy Manual 3-16, "Control of Communications Security Material," January 23, 2015, as amended

United States Code, Title 10, Section 189