DoD INSTRUCTION 8560.01

COMMUNICATIONS SECURITY (COMSEC) MONITORING

Originating Component:	Office of the Chief Information Officer of the Department of Defense
Effective:	August 22, 2018
Releasability:	Cleared for public release. Available on the DoD Issuances Website at http://www.esd.whs.mil/DD/.
Incorporates and Cancels:	DoD Instruction 8560.01, "Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing," October 9, 2007
Approved by:	Dana Deasy, DoD Chief Information Officer

Purpose: In accordance with the authority in DoD Directive 5144.02, this issuance implements National Telecommunications and Information Systems Security Directive (NTISSD) No. 600 by establishing policies and assigining responsibilities for conducting COMSEC monitoring of DoD telecommunications.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) 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").

b. Does not authorize, or otherwise apply to, the monitoring of telecommunications for purposes governed by other DoD policy and guidance. This includes, but is not limited to, monitoring for:

(1) Signals intelligence.

(2) Technical surveillance countermeasures.

(3) Intelligence, surveillance, and reconnaissance in cyberspace.

(4) Surveillance of non-communications emissions (e.g., emissions from radar or telemetry).

(5) Law enforcement, foreign intelligence and counterintelligence purposes.

(6) Network management to administer, operate, and reliably maintain the network systems.

(7) Operational test and evaluation.

(8) Laboratory research and development testing.

(9) TEMPEST testing.

(10) External reviews, independent verification, and validation.

1.2. POLICY. It is DoD policy to:

a. Provide legally sufficient notice to DoD system users of COMSEC monitoring and obtain valid user consent to such monitoring prior to conducting monitoring for COMSEC purposes.

b. Assess the degree to which DoD COMSEC, operations security (OPSEC), and cybersecurity programs protect DoD telecommunications.

c. Assess the susceptibility of information systems to surreptitious intrusion, data manipulation, denial of service, and other offensive information operation attacks. Evaluate the potential impacts associated with these risks.

d. Conduct COMSEC monitoring to assess the type and value of information subject to loss through intercept and exploitation of DoD telecommunications.

e. Provide supporting data on the effectiveness of cybersecurity capabilities to defense readiness reporting.

f. Identify telecommunications signals that exhibit unique external parameters, structures, modulation schemes, or other characteristics that make them potentially susceptible to specific identification and geopositioning or other adverse action.

g. Use the results of COMSEC monitoring to evaluate the effectiveness of associated education and training, and provide supporting data to form the basis for additional education and training.

h. Avoid monitoring any telecommunications or information technology system contents for COMSEC purposes when such monitoring would constitute electronic surveillance.

SECTION 2: RESPONSIBILITIES

2.1. DOD CHIEF INFORMATION OFFICER (DOD CIO). The DoD CIO:

a. Oversees the implementation of this issuance.

b. Develops and publishes additional guidance, consistent with this issuance, in conjunction with the Joint Staff, the National Security Agency, and other DoD Components.

c. Informs the Secretary of Defense and Deputy Secretary of Defense of DoD COMSEC monitoring as appropriate.

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:

a. Facilitates COMSEC monitoring at the DoD telecommunication nodes.

b. Provides DoD information networks bandwidth for data transport from remotely deployed COMSEC monitoring equipment when requested.

2.3. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF CENTRAL SECURITY SERVICE (DIRNSA/CHCSS). Under the authority, direction, and control of the Under Secretary of Defense for Intelligence, and in addition to the responsibilities in Paragraph 2.5, the DIRNSA/CHCSS, acting in the role of National Security Directive-42 National Manager:

a. Serves as the DoD focal point for COMSEC monitoring.

b. Maintains the capability to execute national-level COMSEC monitoring for employment in single Military Service, Joint, and national-level exercises, operations, and other activities, as directed in accordance with DoD Directive 5100.20.

c. Provides COMSEC monitoring services to DoD Components through the Joint Communications Security Monitoring Activity (JCMA).

d. Publishes standardized procedures and safeguards, in coordination with the DoD CIO and other DoD Components, for use throughout the DoD to ensure that COMSEC monitoring is conducted safely, securely, and in accordance with applicable laws, regulations, and policies.

e. Maintains, in coordination with the Under Secretary of Defense for Personnel and Readiness and the Secretaries of the Military Departments, formal training and certification standards, curricula, and related materials for all DoD personnel involved in COMSEC monitoring in accordance with DoD Directive 1322.18.

f. Advises DoD Components regarding COMSEC monitoring, tools, techniques, and procedures through the JCMA.

g. Coordinates with the CJCS to prioritize and organize joint COMSEC monitoring requirements and their execution.

h. Develops processes and procedures to share lessons learned from COMSEC monitoring among DoD Components.

i. Maintains a database of certifications from DoD Components' legal counsel, stating, at a minimum, that users of the component's telecommunications and information systems have been provided legally sufficient notice of monitoring for authorized purposes and that informed user consent to such monitoring has been obtained.

j. Provides information on the availability of National Security Agency/Chief Central Security COMSEC monitoring resources to the CJCS, as required.

2.4. GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE. The General Counsel of the Department of Defense:

a. Provides oversight and guidance on all legal matters pertaining to COMSEC monitoring procedures and activities.

b. Reviews and approves OSD COMSEC monitoring in accordance with this issuance and NTISSD No. 600.

2.5. DOD COMPONENT HEADS The DoD Component heads:

a. Approve DoD Component initiated COMSEC monitoring of DoD Component owned or DoD Component controlled telecommunications systems. Approval authority may be delegated in writing to a designated official.

b. Incorporate COMSEC monitoring and associated training objectives and concepts in joint military and Service education curricula.

c. Certify every 2 years through the DoD Component's legal counsel to the DIRNSA/CHCSS that users of the DoD Component's telecommunications and information systems have been provided legally sufficient notice of monitoring for authorized purposes and that informed user consent to such monitoring has been obtained. This certification responsibility may not be further delegated to a DoD Component's sub-components.

d. Use the standard DoD banner and user agreement, as directed in DoD Instruction 8500.01, to provide legally sufficient notice of monitoring for authorized purposes to users of the DoD Component's telecommunications and information systems and to obtain informed consent to such monitoring from those users.

2.6. SECRETARIES OF THE MILITARY DEPARTMENTS. In addition to the responsibilities in Paragraph 2.5, the Secretaries of the Military Departments:

a. Implement procedures for conducting COMSEC monitoring in coordination with DIRNSA/CHCSS and consistent with this issuance.

b. Ensure those performing COMSEC monitoring:

(1) Receive formal training.

(2) Are fully competent in using the tools, techniques, and procedures associated with such activities, and properly understand their duties and the relevant legal requirements.

c. Ensure their department's general counsel reviews and provides written approval of their department's COMSEC monitoring procedures, training processes, and user notification procedures every 2 years.

(1) These copies of written approvals are provided to the General Counsel of the Department of Defense and the National Security Agency Associate General Counsel/Operational Support, pursuant to NTISSD No. 600.

(2) This responsibility does not absolve the Secretaries of the Military Departments of responsibility under Paragraph 2.5.c. Paragraph 2.6.c delineates a separate, additional responsibility.

d. Share lessons learned from COMSEC monitoring across the DoD consistent with security and operational requirements.

2.7. CJCS. In addition to the responsibilities in Paragraph 2.5, the CJCS:

a. Ensures that Combatant Commanders issue appropriate COMSEC monitoring procedures for all supported operations.

b. Assists the DIRNSA/CHCSS, as required, with the prioritization and coordination of JCMA and Military Service COMSEC monitoring requirements and execution.

c. Provides guidance and oversight to the JCMA.

SECTION 3: COMSEC MONITORING ACTIVITIES

3.1. INTRODUCTION.

a. DoD telecommunications systems are provided for authorized government communications and are subject to COMSEC monitoring.

b. COMSEC monitoring will be conducted in accordance with applicable federal law,the Fourth Ammendment, and in a manner that minimizes the collection of telecommunications content not related to security objectives. This will protect to the greatest extent possible the privacy and civil liberties of individuals whose telecommunications are subject to monitoring.

c. COMSEC monitoring is a vulnerability assessment technique providing essential information not available through other sources of evaluating security within DoD.

3.2. COMSEC MONITORING PURPOSE.

COMSEC monitoring may be undertaken to:

a. Measure the effectiveness of encryption, cryptographic equipment and devices, COMSEC techniques, and OPSEC.

b. Provide a basis to assess the contents and value of information that is subject to loss through exploitation of DoD telecommunications.

c. Provide a basis for improving the security of DoD telecommunications against signals intelligence exploitation.

d. Collect signals or data needed to evaluate the function or security posture of cryptographic equipment and other cybersecurity measures and techniques.

e. Identify system signals or data that exhibit unique external parameters, structures, modulation schemes, or other characteristics that could provide signals intelligence elements of foreign powers the capability to identify specific targets for subsequent geopositioning and exploitation purposes.

f. Obtain OPSEC indicators from DoD telecommunications to support OPSEC surveys.

g. Evaluate the effectiveness of OPSEC, cybersecurity, and COMSEC education and training programs.

3.3. NOTIFICATION.

a. DoD telecommunications and information systems are subject to COMSEC monitoring by duly authorized government entities.

(1) Users of these systems must be properly notified in advance that their use of these systems constitutes consent to monitoring for COMSEC purposes.

(2) The use of such systems by any person shall constitute implied consent to the monitoring for COMSEC purposes of communications carried over them.

(3) DoD shall not monitor telecommunications systems which are owned or leased by DoD contractors for their own use without first obtaining the express written approval of the chief executive officer of the contractor organization (or their designee) and the written opinion of the general counsel of the DoD Component which is actually performing the monitoring that procedures have been implemented sufficiently to afford notice to the contractor organization's employees.

b. Notice of existence of COMSEC monitoring can be accomplished by any of the following means or any combination thereof which the legal counsel of the affected DoD Component considers legally sufficient to achieve proper notification in terms of content, prominence, and specificity:

(1) DoD consent notice displayed on screens upon initial access to telecommunications and information technology devices and access to network connected telecommunications and information technology systems.

(2) Warning banners decals placed on the transmitting or receiving devices.

(3) A notice in the daily bulletin or similar medium.

(4) A specific memorandum to users.

(5) A statement on the cover of the official telephone book or communications directory.

(6) A statement in the standing operating procedures, communications-electronics operating instructions, or similar documents.

3.4. TRAINING AND STANDARDS.

a. All individuals conducting COMSEC monitoring will receive formal training before participating in monitoring activities.

b. For COMSEC monitoring operations, the first O-5 or civilian equivalent in the individual's chain of command will certify, in writing, the individual has been trained. The monitoring unit or organization will maintain a copy of the certification on-file.

c. Personnel participating in COMSEC monitoring will receive mandatory annual refresher training.

d. When required, personnel that have not received formal training may conduct COMSEC monitoring under a supervisor that has been formally trained.

(1) Personnel without formal COMSEC monitoring training must understand the purposes and restrictions applied to COMSEC monitoring operations as detailed in this issuance and NTISSD No. 600.

(2) The use of personnel without formal COMSEC monitoring training must be approved on a case-by-case basis by an individual designated by the head of the organization conducting the monitoring.

3.5. USE OF COMSEC MONITORING RESULTS. COMSEC monitoring will only be used to evaluate the status of COMSEC within DoD.

a. The results of COMSEC monitoring shall not be used to produce foreign intelligence or counter intelligence. The results of COMSEC monitoring of exercise communications may be used for exercise intelligence purposes.

b. DoD Components many not monitor the telecommunications and information technology of another component for COMSEC purposes without the express prior written approval of the head (or their designee) of the component to be monitored, except as necessary in order to perform Director, National Security Agency, responsibilities.

c. Information acquired incidentally from DoD telecommunications and information technology during the course of authorized COMSEC monitoring which relates directly to a significant crime will be referred to the military commander or law enforcement agency having appropriate jurisdiction and:

(1) The general counsel of the DoD Component which is actually performing the COMSEC monitoring shall be notified promptly.

(2) The results of COMSEC monitoring may not be used in a criminal prosecution without prior consultation with the general counsel of the DoD Component which actually performed the monitoring.

GLOSSARY

G.1. ACRONYMS.

CJCS	Chairman of the Joint Chiefs of Staff
COMSEC	communications security
DIRNSA/CHCSS	Director, National Security Agency/Chief Central Security Service
DoD CIO	DoD Chief Information Officer
JCMA	Joint Communications Security Monitoring Activity
NTISSD	National Telecommunications and Information Systems Security Directive
OPSEC	operations security

G.2. DEFINITIONS. Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

COMSEC. Defined in Committee on National Security Systems Instruction No. 4009.

COMSEC monitoring. Defined in NTISSD No. 600.

contents. Defined in NTISSD No. 600.

cryptographic equipment. Defined in Committee on National Security Systems Instruction 4009.

cybersecurity. Defined in DoD Dictionary of Military and Associated Terms.

DoD Information Network. Defined in DoD Dictionary of Military and Associated Terms.

node. Defined in DoD Dictionary of Military and Associated Terms.

OPSEC. Defined in DoD Dictionary of Military and Associated Terms.

readiness. Defined in DoD Dictionary of Military and Associated Terms.

technical surveillance countermeasures. Defined in DoD Dictionary of Military and Associated Terms.

telecommunications. Defined in NTISSD No. 600.

telecommunications systems. Defined in NTISSD No. 600.

TEMPEST. Defined in NTISSD No. 4009.

REFERENCES

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

DoD Directive 1322.18, "Military Training," January 13, 2009, as amended

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

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

DoD Instruction 8500.01, "Cybersecurity," March 15, 2014

National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990

National Telecommunications and Information Systems Security Directive No. 600, "Communications Security (COMSEC) Monitoring," April 10, 1990

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