Department of Defense

# INSTRUCTION

**NUMBER** 8560.01
October 9, 2007

ASD(NII)/DoD CIO

SUBJECT: Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing

References: (a) DoD Directive 4640.6, "Communications Security Telephone Monitoring and Recording," June 26, 1981 (hereby canceled)
(b) Acting Deputy Secretary of Defense Memorandum, "DoD Directives Review – Phase II," July 13, 2005
(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) National Telecommunications and Information Systems Security Directive No. 600, "Communications Security (COMSEC) Monitoring," April 10, 1990[1]
(e) through (i), see Enclosure 1

1. PURPOSE

This Instruction:

1.1. Reissues Reference (a), as a DoD Instruction, under a new number and title, in accordance with the guidance in Reference (b) and the authority in Reference (c).

1.2. Implements Reference (d) by establishing DoD policies and responsibilities for conducting COMSEC monitoring of DoD telecommunications systems.

1.3. Establishes and implements DoD policies and responsibilities for conducting IA readiness testing of operational DoD information systems in accordance with DoD Directive 8500.1 (Reference (e)).

1.4. Authorizes the monitoring of DoD telecommunications systems for COMSEC purposes and the penetration of DoD information systems for IA readiness testing purposes only.

[1] Available at http://www.iad.nsa.smil.mil/resources/library

2. APPLICABILITY AND SCOPE

This Instruction:

2.1. Applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of 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"). The term "Military Services," as used herein, refers to the Army, the Navy, the Air Force, and the Marine Corps.

2.2. This Instruction does not authorize, or otherwise apply to, the monitoring of telecommunications systems or testing of DoD information systems for purposes governed by other DoD policy and guidance. This includes, but is not limited to, monitoring or testing for:

2.2.1. Administration and management functions to ensure proper installation, integration, and functioning of equipment and systems (e.g., certification and accreditation activities, internal reviews, connection approvals).

2.2.2. Signals intelligence.

2.2.3. Technical surveillance countermeasures.

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

2.2.5. Laboratory research and development testing.

2.2.6. Operational test and evaluation.

2.2.7. Foreign intelligence and counterintelligence purposes.

2.2.8. TEMPEST testing.

2.2.9. Law enforcement purposes.

2.2.10. External reviews and/or independent verification and validation (IV&V).

3. DEFINITIONS Terms used in this Instruction are defined in Enclosure 2 and Joint Publication 1-02 (Reference (f)).

4. POLICY

It is DoD policy to:

4.1. Conduct COMSEC monitoring activities of DoD telecommunications systems and IA readiness testing of DoD information systems only when authorized by the Head of a DoD Component as a means to:

4.1.1. Assess the contents and value of government information that is subject to loss or exploitation by way of telecommunications and information systems.

4.1.2. Collect signals needed to evaluate the function or security posture of cryptographic equipment and other IA measures and techniques.

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

4.1.4. 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.

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

4.2. Comply with DoD Directive 8500.1, Executive Order 12333 as amended, National Security Directive 42, and the Chairman of the Joint Chiefs of Staff Manual 6510.01 (References (e), (g), (h) and (i) respectively); as well as all other applicable laws, Executive Orders, DoD Issuances, and this Instruction, when conducting COMSEC monitoring and IA readiness testing.

4.3. Require the written approval of the Head of a DoD Component or an authorized designee, or the approval of the Secretary or Deputy Secretary of Defense before commencing actual COMSEC monitoring or IA readiness testing of systems owned or leased by the Department of Defense, in accordance with Reference (d). COMSEC monitoring or IA readiness testing of contractor organizations requires the additional approval of the organization's chief executive officer or an authorized designee.

4.4. Provide authorized users of DoD telecommunications systems and DoD information systems with legally sufficient notice that their use of these systems constitutes consent to monitoring for all authorized purposes.

4.5. Conduct COMSEC monitoring and IA readiness testing in a manner that minimizes, consistent with operational requirements, intercepting or recording the contents of communications or information not relevant to the mission. Information incidentally acquired as part of an authorized COMSEC monitoring or IA readiness testing operation - that directly relates to a significant crime - shall be referred to the Military Commander, DoD Component Head, or law enforcement agency with jurisdiction over the offense, as required by applicable statutes, policies, regulations, and other agreements. When taking such action, the general

counsel of the department or agency which is actually performing the COMSEC monitoring shall be notified promptly. The results of COMSEC monitoring may not be used in a criminal prosecution without prior consultation with the general counsel of the department or agency which actually performed the monitoring. Any subsequent DoD electronic surveillance arising from this information shall only be conducted in accordance with DoD 5240.1-R (Reference (j)) or DoD Directive 5505.9 (Reference (k)), whichever is appropriate.

4.6. Avoid permanent damage, destruction, or degradation of DoD information systems or facilities during IA readiness testing unless the approved objectives of the exercise specifically authorize such consequences.

4.7. Except as otherwise provided herein, information acquired for COMSEC purposes shall only be retained so long as is absolutely necessary to accomplish the COMSEC objectives and while retained will be afforded protection commensurate with its classification or sensitivity.

## 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 the implementation of this Instruction.

5.1.2. Develop and promulgate, in conjunction with the Joint Staff, associated Military Services, and agencies, any additional DoD guidance consistent with this Instruction.

5.1.3. Inform the Secretary and Deputy Secretary of Defense of DoD COMSEC monitoring and IA readiness testing activities as appropriate.

5.2. The Director, Defense Information Systems Agency, under the authority, direction, and control of the ASD(NII)/DoD CIO, shall:

5.2.1. Provide access to the Global Information Grid (GIG) topology and architecture in support of COMSEC monitoring and IA readiness testing.

5.2.2. Facilitate COMSEC monitoring and IA readiness testing at the GIG nodes.

5.2.3. Provide GIG bandwidth for data transport from remotely deployed COMSEC monitoring equipment when requested.

5.3. The Director, Defense Intelligence Agency, under the authority, direction, and control of the Under Secretary of Defense for Intelligence (USD(I)), shall provide the Heads of the DoD Components tailored intelligence support for the development of realistic threat assessments to DoD information systems when requested.

5.4. The Director, National Security Agency (DIRNSA) under the authority, direction, and control of the USD(I), shall serve as the DoD focal point for COMSEC monitoring and IA readiness testing and shall:

5.4.1. Provide COMSEC monitoring services to the Department of Defense and other U.S. Government departments and agencies through the Joint COMSEC Monitoring Activity (JCMA), National Security Agency (NSA)/Central Security Service (CSS) Threat Operations Center (NTOC), and the Military Service Cryptologic Elements.

5.4.2. Develop and maintain a capability to execute national-level COMSEC monitoring and IA readiness testing efforts for employment in single Military Service, Joint, and national-level exercises, operations, and other activities, as directed. Authorization for NSA participation in IA readiness testing of an information system or network shall include authorization for NSA personnel involved in the readiness testing to use any information system not specifically prohibited that is owned or leased by the Department of Defense as a point of entry or "jump point" into the system or network that is the primary target of the IA readiness testing.

5.4.3. Develop and promulgate standardized procedures and safeguards, in coordination with ASD(NII)/DoD CIO and other DoD Components designated by ASD(NII)/DoD CIO, for use throughout the Department of Defense to ensure that COMSEC monitoring and IA readiness testing is conducted safely, securely, and in accordance with applicable laws, regulations and policies.

5.4.4. Develop and maintain, in coordination with the Military Services, formal training and certification standards, curricula, and related materials for all DoD personnel involved in COMSEC monitoring and IA readiness testing.

5.4.5. Act as a consultant to DoD Components and other U.S. Government departments and agencies regarding COMSEC monitoring and IA readiness testing tools, techniques, and procedures.

5.4.6. Advise and assist other DoD Components, as requested, in implementing this Instruction.

5.4.7. Coordinate with the Chairman of the Joint Chiefs of Staff to prioritize and organize COMSEC monitoring requirements and their execution.

5.4.8. In coordination with the Chairman of the Joint Chiefs of Staff, the Commander of the U.S. Strategic Command, and the Military Services, develop processes and procedures to share lessons learned from COMSEC monitoring and IA readiness testing missions across the Department of Defense, while ensuring the anonymity of DoD Components consistent with security and operational requirements.

5.4.9. Establish and maintain a database of certifications from the Heads of the DoD Components that state users of the DoD Component's information systems are provided legally

sufficient notice that use of those systems constitutes consent to monitoring for authorized purposes. Ensure that such certifications fully meet the intent of Reference (d).

5.5. The General Counsel of the Department of Defense (GC, DoD) shall:

5.5.1. Provide oversight and guidance on all legal matters pertaining to COMSEC monitoring and IA readiness testing procedures and activities.

5.5.2. Review and approve OSD monitoring in accordance with this Instruction and Reference (d).

5.6. The Heads of the DoD Components shall:

5.6.1. Approve DoD Component-initiated COMSEC monitoring and IA readiness testing of DoD Component-owned or leased systems. Approval may also be granted by designee appointed in writing.

5.6.2. Use the standard DoD banner and user agreement language as issued to inform users of DoD information systems that use of such systems constitutes a consent to monitoring for all authorized purposes.

5.6.3. Incorporate COMSEC monitoring, IA readiness testing, and associated training objectives and concepts in joint military and Service education curricula.

5.6.4. In accordance with Reference (d), certify biennially through the DoD Component's legal counsel to the DIRNSA, as the National Manager for Telecommunications and Automated Information Systems Security, that users of the DoD Component's telecommunications systems and information systems are provided legally sufficient notice that use of those systems constitutes a consent to monitoring for all authorized purposes.

5.6.5. Ensure planned DoD Component IA readiness testing is coordinated with the U.S. Strategic Command (USSTRATCOM) and NSA.

5.7. The Secretaries of the Military Departments shall:

5.7.1. In coordination with the DIRNSA, implement procedures for conducting COMSEC monitoring and IA readiness testing consistent with this Instruction.

5.7.2. Ensure that those performing COMSEC monitoring and IA readiness testing receive formal training, are fully competent in using the tools, techniques, and procedures associated with such activities, and properly understand their duties and the relevant legal requirements.

5.7.3. Ensure that their Department's General Counsel reviews and provides written approval of their Department's COMSEC monitoring and IA readiness testing procedures, training processes, and user notification procedures on a biennial basis, and that copies of such

written approvals are provided to the GC, DoD, and the NSA Associate General Counsel for IA, as required by Reference (d).

5.7.4. Ensure that IA readiness testing activities support Computer Network Defense (CND) and are coordinated in advance with the USSTRATCOM Joint Task Force-Global Network Operations, other CND service providers, and law enforcement agencies as appropriate.

5.7.5. Consistent with security and operational requirements, share lessons learned from COMSEC monitoring and IA readiness testing missions across the Department of Defense.

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

5.8.1. Ensure that Combatant Commanders promulgate appropriate COMSEC monitoring and IA readiness testing procedures for support to Joint, combined, and single Service operations.

5.8.2. Assist the DIRNSA, as required, with the prioritization and coordination of JCMA and Military Service COMSEC monitoring requirements and execution.

5.8.3. Provide guidance and oversight to the JCMA.

5.9. The Commander of the USSTRATCOM, through the Chairman of the Joint Chiefs of Staff, shall:

5.9.1. Develop procedures and direct technical implementation for countermeasures resulting from IA readiness testing.

5.9.2. Coordinate and, when required, direct IA readiness testing of the GIG.

## 6. 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 8500.1, "Information Assurance (IA)," October 24, 2002
(f) Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms," as amended
(g) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended[2]
(h) National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990[3]
(i) Chairman of the Joint Chiefs of Staff Manual 6510.01, "Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)," March 5, 2003
(j) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 1982
(k) DoD Directive 5505.9, "Interception of Wire, Electronic, and Oral Communication for Law Enforcement," April 20, 1995

[2] Available at http://www.iad.nsa.smil.mil/resources/library
[3] Available at http://www.iad.nsa.smil.mil/resources/library

# E2. ENCLOSURE 2

## DEFINITIONS

E2.1. Communications Security (COMSEC). See Reference (f).

E2.2. Communications Security (COMSEC) Monitoring. See Reference (f).

E2.3. Computer Network Defense (CND). For the purpose of this Instruction, CND is actions taken under legal authority to protect, monitor, analyze, detect, and respond to unauthorized activity in DoD information systems and computer networks. Unauthorized activity may include disruption, denial, degradation, destruction, exploitation, or access to computer networks, information systems or their contents, or theft of information. CND protection activity employs IA protection activity and includes deliberate actions taken to modify an assurance configuration or condition in response to a CND alert or threat information. Monitoring, analysis, and detection activities, including trend and pattern analysis, are performed by multiple disciplines in the Department of Defense (e.g., network operations, intelligence, counterintelligence, and law enforcement).

E2.4. Contents. See Reference (d).

E2.5. Cryptographic Equipment. Equipment that embodies a cryptographic logic, i.e., one or more crypto-algorithm(s) along with alarms, checks, and other processes essential to effective and secure performance of the cryptographic process(es).

E2.6. Denial of Service. Any action or series of actions that prevents any part of an information system from functioning.

E2.7. Global Information Grid (GIG). See Reference (f).

E2.8. Information Assurance (IA). See Reference (f).

E2.9. Information Assurance (IA) Readiness Testing. Identification, exposure, and possible exploitation of information system vulnerabilities by simulating a malicious attack to penetrate or gain access to a system or network. This testing is done to aid in evaluating the IA posture of an organization. Also known as “penetration testing,” and is employed during “Red Team” assessments and may be employed as part of “Blue Team” assessments.

E2.10. Intrusion. Unauthorized act of bypassing the security mechanisms of a system.

E2.11. Penetration Testing. Security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation.

E2.12. Technical Surveillance Countermeasures. See Reference (f).

E2.13. Telecommunications Systems. For the purpose of this Instruction, telecommunications systems are interconnected devices used to transmit, receive, or process telecommunications. The devices may be electrical, electromagnetic, electromechanical, or electro-optical. Telecommunication systems include, but are not limited to, conventional telephones, satellite telephones, cellular telephones, computer-based transmission systems, facsimile machines, paging devices, and tactical radio systems.

E2.14. TEMPEST. See Reference (f).

E2.15. TEMPEST Test. Laboratory or on-site test to determine the nature of compromising emanations associated with an information system, device or component.

E2.16. Threat Assessment. Formal description and evaluation of threat to an information system.