Department of Defense

INSTRUCTION

NUMBER 5205.08
November 8, 2007

USD(I)

SUBJECT: Access to Classified Cryptographic Information

References: (a) DoD Directive 5205.8, subject as above, February 20, 1991 (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) National Telecommunications and Information Systems Security Policy (NTISSP) No. 3, "National Policy for Granting Access to U.S. Classified Cryptographic Information," December 19, 1988 (FOUO)
(e) through (j), see Enclosure 1

1. REISSUANCE AND PURPOSE

This Instruction:

1.1. Reissues Reference (a) as a DoD Instruction in accordance with the guidance in Reference (b) and the authority of Reference (c).

1.2. Updates the policies and responsibilities for the program established under Reference (d) to govern the granting of access to United States (U.S.) classified cryptographic information that is owned, controlled, and produced by or for the Department of Defense.

2. APPLICABILITY AND SCOPE

This Instruction:

2.1. Applies to the Office of the Secretary of Defense, 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 within the Department of Defense (hereafter referred to collectively as the "DoD Components").

2.2. Applies to all members of the U.S. Armed Forces, civilian employees of the Department of Defense and, consistent with DoD 5220.22-R (Reference (e)), contractors, consultants, and other persons employed by or affiliated with the Department of Defense who have access to classified U.S. cryptographic information and whose duties require continuing access thereto. (See section 3.) Accordingly, this Instruction applies to those persons assigned:

2.2.1. As cryptographic material custodians, alternates, or their equivalents.

2.2.2. As cryptographic key or logic producers or developers.

2.2.3. As cryptographic maintenance, engineering, or installation technicians.

2.2.4. To supply points where cryptographic keying materials are generated or stored, and to those having access to such materials.

2.2.5. To secure telecommunications facilities located on the ground, on board ship, or on communications support aircraft and whose duties require keying of cryptographic equipment.

2.2.6. To prepare, authenticate, or decode nuclear control orders (valid or exercise).

2.2.7. To any other responsibility requiring or enabling access to classified cryptographic media.

2.3. Does not apply to individuals whose duties are to operate (but not to key or maintain) systems using cryptographic equipment.

2.4. Excludes controlled cryptographic items as defined in NTISSI No. 4001 (Reference (f)).

2.5. Shall not alter existing authorities of the Director of National Intelligence under Executive Order 12333 (Reference (g)).

3. DEFINITIONS

For the purpose of this Instruction, classified cryptographic information is defined as:

3.1. Cryptographic keys and authenticators that are classified under DoD 5200.1-R (Reference (h)) and designated as SECRET CRYPTO or TOP SECRET CRYPTO.

3.2. Classified cryptographic media that embody, describe, or implement a classified cryptographic logic, to include (but not be limited to) full maintenance manuals, cryptographic descriptions, drawings of cryptographic logic, specifications describing a cryptographic logic, and cryptographic software, firmware, or repositories of such software (e.g., magnetic media or optical disks.

4. POLICY

It is DoD policy that a person may be granted access to classified cryptographic information, as specified in sections 2 and 3, only if that person:

4.1. Is a U.S. citizen.

4.2. Is a civilian employee of the Department of Defense, a member of the U.S. Armed Forces, a DoD-cleared contractor or employee of such contractor, or is employed as a DoD representative (including consultants of the Department of Defense).

4.3. Requires access to perform official duties for or on behalf of the Department of Defense.

4.4. Possesses a security clearance appropriate to the level of classification of the cryptographic information to be accessed, in accordance with DoD 5200.2-R (Reference (i)).

4.5. Receives a security briefing appropriate to the cryptographic information to be accessed.

4.6. Acknowledges the granting of access by signing a cryptographic access certificate.

4.7. Agrees to report foreign travel and any form of contact with foreign nationals, in accordance with Reference (i).

4.8. Acknowledges the possibility of being subject to a counterintelligence scope polygraph examination administered in accordance with DoD Directive 5210.48 (Reference (j)).

5. RESPONSIBILITIES

5.1. The Under Secretary of Defense for Intelligence (USD(I)) shall oversee and review the implementation of this Instruction.

5.2. The Heads of the DoD Components shall:

5.2.1. Control access to classified cryptographic information in accordance with section 4.

5.2.2. Carry out and administer a cryptographic access program within their respective organizations. This program shall include cryptographic access briefings and execution of cryptographic access certificates. (See Enclosure 2 and SD Form 572, "Cryptographic Access Certification and Termination."[1])

5.2.3. In accordance with Reference (j), carry out a counterintelligence scope polygraph examination program in support of this Instruction.

[1] Found at: http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfopage2004.html

5.2.4. Maintain records on all individuals who have been granted cryptographic access or have had their cryptographic access withdrawn. Arrange for retention of cryptographic access certificates or legally enforceable facsimiles in accordance with the DoD Component records disposition schedules.

5.2.5. Accept as valid the cryptographic access granted by other DoD Components.

5.2.6. Deny or withdraw cryptographic access to those individuals who fail to agree to or comply with the specific criteria identified in section 4.

5.2.7. Incorporate this policy into appropriate training and awareness programs.

6. EFFECTIVE DATE

This Instruction is effective immediately.

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

Enclosures - 2
E1. References, continued
E2. Sample - Cryptographic Access Briefing

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD 5220.22-R, "Industrial Security Regulation," December 1985
(f) National Telecommunications and Information Systems Security Instruction (NTISSI) No. 4001, "Controlled Cryptographic Items," July 1996 (FOUO)
(g) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
(h) DoD 5200.1-R, "Information Security Program," January 1997
(i) DoD 5200.2-R, "Personnel Security Program," January 1987
(j) DoD Directive 5210.48, "Polygraph and Credibility Assessment Program," January 25, 2007

E2. ENCLOSURE 2

SAMPLE - CRYPTOGRAPHIC ACCESS BRIEFING

You have been selected to perform duties that will require access to classified cryptographic information. It is essential that you be made aware of certain facts relevant to the protection of this information before access is granted. You must know the reason why special safeguards are required to protect classified cryptographic information. You must understand the directives that require these safeguards and the penalties you may incur for the unauthorized disclosure and/or retention or negligent handling of classified cryptographic information under the criminal laws of the United States. Failure to properly safeguard this information could cause exceptionally grave damage or irreparable injury to the national security of the United States or could be used to advantage by a foreign nation.

Classified cryptographic information is especially sensitive because it is used to protect other classified information. Any particular piece of cryptographic keying material and any specific cryptographic technique may be used to protect a large quantity of classified information during transmission. If the integrity of the cryptographic system is breached at any point, all information protected by the system may be compromised. The safeguards placed on classified cryptographic information are a necessary component of Government programs to ensure that our Nation's vital secrets are not compromised.

Because access to classified cryptographic information is granted on a strict need-to-know basis, you will be given access to only that cryptographic information necessary in the performance of your duties. You are required to become familiar with (insert, as appropriate, Department or Agency implementing directives covering the protection of cryptographic information). Cited directives are attached in a briefing book for your review at this time.

Especially important to the protection of classified cryptographic information is the immediate reporting of any known or suspected compromise of this information to (insert appropriate security office). If a cryptographic system is compromised but the compromise is not reported, the continued use of the system can result in the loss of all information protected by it. If the compromise is reported, steps can be taken to lessen an adversary's advantage gained through the compromise of the information.

As a condition of access to classified cryptographic information, you must acknowledge that you may be subject to a counterintelligence scope polygraph examination. This examination will be administered in accordance with DoD Directive 5210.48 and applicable law. The relevant questions in this polygraph examination concern espionage, sabotage, unauthorized disclosure of classified information, and unreported foreign contacts. If at this time you do not wish to sign such an acknowledgment as a part of executing a cryptographic access certification, this briefing will be terminated and the briefing administrator will so annotate the cryptographic access certificate. Such refusal will not be cause for adverse action, but will result in your being denied access to classified cryptographic information.

Intelligence services of some foreign governments prize the acquisition of classified cryptographic information. They will go to extreme lengths to compromise U.S. citizens and force them to divulge cryptographic techniques and materials that protect the Nation's secrets around the world. Any personal or financial relationship with a foreign government's representative could make you vulnerable to attempts at coercion to divulge classified cryptographic information. Learn to recognize those attempts so that you may successfully counter them. The best personal policy is to avoid discussions that reveal your knowledge of, or access to, classified cryptographic information and thus avoid highlighting yourself to those who would seek the information you possess. Any attempt, either through friendship or coercion, to solicit your knowledge regarding classified cryptographic information must be reported immediately to (insert appropriate security office).

In view of the risks noted above, unofficial travel to foreign countries may require the prior approval of (insert appropriate security office). It is essential that you contact (insert appropriate security office) before such unofficial travel.

Finally, should you willfully or negligently disclose to any unauthorized persons any of the classified cryptographic information to which you will have access, you may be subject to administrative and civil sanctions, including adverse personnel actions, as well as criminal sanctions under the Uniform Code of Military Justice and/or the criminal laws of the United States, as appropriate.