# DoD INSTRUCTION 5205.08

# ACCESS TO U.S. CLASSIFIED CRYPTOGRAPHIC INFORMATION

| | |
|---|---|
| **Originating Component:** | Office of the Under Secretary of Defense for Intelligence |
| **Effective:** | February 16, 2018 |
| **Releasability:** | Cleared for public release. Available on the DoD Issuances Website at http://www.dtic.mil/whs/directives. |
| **Reissues and Cancels:** | DoD Instruction 5205.08, "Access To Classified Cryptographic Information," November 8, 2007 |
| **Approved by:** | Joseph D. Kernan, Under Secretary of Defense for Intelligence |

**Purpose:** In accordance with the authority in DoD Directive 5143.01, and pursuant to Committee on National Security Systems Policy No. 3, this issuance establishes policy and assigns responsibilities to govern granting access to U.S. classified cryptographic information that is owned, controlled, and produced by or for the DoD.

# TABLE OF CONTENTS



FIGURES

# SECTION 1: GENERAL ISSUANCE INFORMATION

**1.1. APPLICABILITY.** This issuance:

a. Applies to:

(1) 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 within the DoD (referred to collectively in this issuance as the "DoD Components").

(2) All Service members and civilian employees of the DoD, and, consistent with DoD 5220.22-M, all DoD-cleared contractors, who pursuant to the terms and conditions of the applicable contract or agreement have access to U.S. classified cryptographic information, and whose duties require continuing access to that information, including, but not limited to, those who are assigned:

(a) As cryptographic material Communications Security Account Managers and Key Management Infrastructure Operational Account Managers, or their alternates or equivalents;

(b) As cryptographic key or logic producers or developers;

(c) As cryptographic maintenance, engineering, or installation technicians;

(d) To supply points where cryptographic keying materials are generated or stored, and to those having access to such materials;

(e) To secure telecommunications facilities located on the ground, on board ship, or on communications support aircraft and whose duties require keying of cryptographic equipment;

(f) To prepare, authenticate, or decode nuclear control orders (valid or exercise); or

(g) To any other responsibility requiring or enabling access to classified cryptographic media.

b. Does not apply to:

(1) Individuals whose duties are to operate, but not to key or maintain, systems using cryptographic equipment; and

(2) Controlled cryptographic items as defined in Committee on National Security Systems Instruction (CNSSI) No. 4001.

c. Does not alter any existing authorities of the Director of National Intelligence, including under Executive Order 12333.

**1.2. POLICY.** It is DoD policy that a person may be granted access to U.S. classified cryptographic information in accordance with this issuance only if that person:

a. Is a U.S. citizen.

b. Is a Service member, DoD civilian employee, or a DoD-cleared contractor.

c. Requires access to perform official duties for or on behalf of the DoD.

d. Possesses a security clearance appropriate to the level of classification of the cryptographic information to be accessed, in accordance with DoD Instruction 5200.02 and DoD Manual 5200.02.

e. Satisfies all requirements in Section 3.

# SECTION 2: RESPONSIBILITIES

**2.1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE.** The Under Secretary of Defense for Intelligence oversees the implementation of this issuance.

**2.2. DOD COMPONENT HEADS.** The DoD Component heads:

a. Control access to U.S. classified cryptographic information in their control or possession, and their facilities containing U.S. classified cryptographic information, in accordance with this issuance, DoD Instruction 5200.08, DoD 5200.08-R, and Directive-type Memorandum 09-012, as applicable.

b. Administer U.S. classified cryptographic information access programs within their respective Components, including conducting U.S. classified cryptographic information access briefings and ensuring completion of relevant documentation, including Secretary of Defense (SD) Form 572, "Cryptographic Access Certification and Termination."

c. Administer a counterintelligence scope polygraph examination program within their respective Components in accordance with DoD Directive 5210.48.

d. Maintain records on all individuals who have been granted access to U.S. classified cryptographic information, or have had their access to U.S. classified cryptographic information withdrawn in accordance with applicable law, regulation, and policy, including. e.g., Section 552a of Title 5, United States Code (also known as "The Privacy Act of 1974"), DoD 5400.11-R, DoD Directive 5400.11, and DoD Instruction 5015.02.

e. Retain originally signed cryptographic access certificates or legally enforceable certified copies, in accordance with their respective DoD Components' records disposition schedule(s).

f. Accept as valid the access to U.S. classified cryptographic information granted by other DoD Components.

g. Deny or withdraw access to U.S. classified cryptographic information to those individuals who fail to comply with the procedures in Section 3.

h. Incorporate this issuance into appropriate DoD Component training and awareness programs.

## SECTION 3: PROCEDURES FOR GRANTING ACCESS

A DoD Component head, or his or her designee, may grant access to U.S. classified cryptographic information to a person referred to in Paragraph 1.2., only if that person:

a. Receives a security briefing appropriate to the cryptographic information to be accessed (see Figure 1).

b. Signs a SD 572, "Cryptographic Access Certification and Termination," cryptographic access certificate acknowledging access granted.

c. Agrees to report foreign travel and any form of contact with foreign nationals, in accordance with DoD Instruction 5200.02, DoD Directive 5240.06, and DoD Manual 5200.02.

d. Agrees to be subject to counterintelligence scope polygraph examinations, as appropriate, which are administered in accordance with DoD Directive 5210.48.

**Figure 1. Sample Cryptographic Access Briefing**

You have been selected to perform duties that will require access to classified cryptographic information. Before access is granted you must be aware of certain facts relevant to the protection of this information. You must know the reason 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, 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, or groups hostile to the Unites States and its allies.

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 classified cryptographic information necessary to the performance of your duties. You are required to become familiar with [insert appropriate Department or Agency implementing guidance covering the protection of cryptographic information]. These documents 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 classified 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.

**Figure 1. Sample Cryptographic Access Briefing, Continued**

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, "Credibility Assessment (CA) Program," 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. Refusal will not be cause for adverse action, but will result in you 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 classified 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 exposing yourself to those who would seek the information you possess. Report any attempt, either through friendship or coercion, to solicit your knowledge regarding classified cryptographic information 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 or the criminal laws of the United States, as appropriate.

# GLOSSARY

**access.** Defined in CNSSI No. 4009.

**authenticate.** Defined in CNSSI No. 4009.

**decode.** Defined in CNSSI No. 4009.

**keying material.** Defined in CNSSI No. 4009.

**U.S. classified cryptographic information.** Defined in CNSS Policy No. 3.

# REFERENCES

Committee on National Security Systems Instruction No. 4001, "Controlled Cryptographic Items," May 7, 2013[1]

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

Committee on National Security Systems Policy No. 3, "National Policy on Granting Access to U.S. Classified Cryptographic Information," October 2007

Directive-type Memorandum 09-012, "Interim Policy Guidance for DoD Physical Access Control," December 8, 2009, as amended

DoD 5200.08-R, "Physical Security Program," April 9, 2007, as amended

DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006, as amended

DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," October 24, 2014, as amended

DoD Directive 5210.48, "Credibility Assessment (CA) Program," April 24, 2015, as amended

DoD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011, as amended

DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

DoD Instruction 5200.02, "DoD Personnel Security Program (PSP)," March 21, 2014, as amended

DoD Instruction 5200.08, "Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)," December 10, 2005, as amended

DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012

DoD Manual 5200.02, "Procedures for the DoD Personnel Security Program (PSP)," April 3, 2017

Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended

United States Code, Title 5, Chapter 5, Section 552a (also known as "The Privacy Act of 1974")

[1] This document is designated FOUO. Please contact the Committee on National Security Systems office to obtain a copy at https://www.cnss.gov