Department of Defense
INSTRUCTION

NUMBER 5210.45
November 14, 2008

USD(I)

SUBJECT: Personnel Security Policies and Procedures for Sensitive Cryptologic Information in the National Security Agency/Central Security Service

References: See Enclosure 1

1. PURPOSE. This Instruction:

a. Reissues DoD Directive (DoDD) 5210.45 (Reference (a)) as a DoD Instruction (DoDI) in accordance with the guidance in DoDI 5025.01 (Reference (b)) and updates policies and responsibilities under the authority in DoDD 5143.01 (Reference (c)).

b. Prescribes the personnel security policies and procedures for the protection of sensitive cryptologic information at the National Security Agency (NSA)/Central Security Service (CSS) in accordance with Chapter 23 of title 50, U.S. Code (Reference (d)).

2. APPLICABILITY. This Instruction applies to:

a. The Office of the Secretary of Defense, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security in agreement with that Department), 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 Department of Defense (hereafter referred to collectively as the "DoD Components").

b. All persons employed by, detailed, or assigned to the NSA/CSS, and to all other persons under the security cognizance of the Director, NSA/Chief, CSS, (DIRNSA/CHCSS) for initial or continued access to sensitive cryptologic information.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. All military and civilian positions of the NSA/CSS are designated as critical sensitive positions and will be treated as such in connection with investigative, personnel security eligibility, and employment matters in accordance with DoDD 5100.23 (Reference (e)).

b. All NSA/CSS employees, contractors, military assignees, and others with similar affiliations with the NSA/CSS must maintain personnel security eligibility for Sensitive Compartmented Information (SCI) for access to sensitive cryptologic information. Eligibility for SCI is a mandatory condition of employment, detail, or assignment at the NSA/CSS.

c. All contracts requiring access to SCI will conform to the requirements of the Federal Acquisition Regulation (Reference (f)).

d. No person shall be employed by, detailed, or assigned to the NSA/CSS, and no person shall have access to classified information of the NSA/CSS, unless:

(1) He or she has been the subject of a full field investigation in connection with such employment, detail, or assignment, and is cleared for access to classified information, and

(2) Such employment, detail, assignment, or access to classified information is clearly consistent with the national security. Any doubt shall be resolved in favor of the national security.

5. RESPONSIBILITIES

a. The Under Secretary of Defense for Intelligence (USD(I)), in accordance with Reference (c), shall exercise oversight of the DIRNSA/CHCSS regarding personnel security policies and procedures for the protection of SCI.

b. The DIRNSA/CHCSS, under the authority, direction, and control of the USD(I) and as a designated head of an element of the Intelligence Community (IC), in accordance with Executive Order (E.O.) 12333 (Reference (g)), shall:

(1) Establish, direct, and administer all aspects of the NSA/CSS personnel security program in accordance with Director of National Intelligence personnel security policies consistent with E.O. 12968 (Reference (h)), and contained in DoD Regulation 5200.2-R (Reference (i)) and IC Directive Number 704 (Reference (j)) as appropriate.

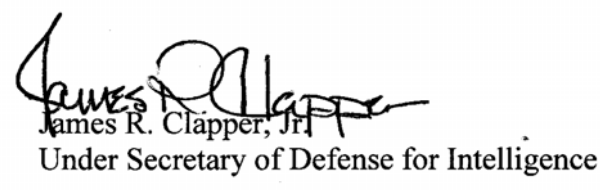
(2) Prepare implementing guidance for the NSA/CSS personnel security program to meet the standards set forth in this Instruction.

c. The DIRNSA/CHCS shall appoint one or more boards of appraisal to perform duties as directed in Reference (d).

6. PROCEDURES. See Enclosure 2.

7. RELEASABILITY. UNLIMITED. This Instruction is approved for public release. Copies may be obtained through the Internet from the DoD Issuances Web Site at http://www.dtic.mil/whs/directives.

8. EFFECTIVE DATE. This Instruction is effective immediately.



Enclosures
1. References
2. Procedures

Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5210.45, "Personnel Security in the National Security Agency," May 9, 1964 (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) Subchapter III, Chapter 23, title 50 of United States Code
(e) DoD Directive 5100.23, "Administrative Arrangements for the National Security Agency," May 17, 1967
(f) Federal Acquisition Regulation, subpart 4.4, current edition
(g) Executive Order 12333, "United States Intelligence Activities," as amended
(h) Executive Order 12968, "Access to Classified Information," as amended
(i) DoD Regulation 5200.2-R, "Personnel Security Program," January 1987
(j) Intelligence Community Directive Number 704, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information," October 1, 2008
(k) DoD Regulation 5210.48-R, "Department of Defense Polygraph Program," January 9, 1985
(l) Office of Management and Budget Memorandum, "Reciprocal Recognition of Existing Personnel Security Clearances," December 15, 2005
(m) Office of Management and Budget, M-06-21, "Reciprocal Recognition of Existing Personnel Security Clearances," July 17, 2006
(n) Executive Order 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information," June 30, 2008
(o) Executive Order 12958, "Classified National Security Information," as amended
(p) Executive Order 12951, "Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems," February 22, 1995
(q) Section 2011, title 42 of United States Code

ENCLOSURE 2

PROCEDURES

1. Personnel security procedures are set forth in Reference (i) and requirements for SCI access are set forth in Reference (j).

2. When the DIRNSA/CHCSS is the cognizant head of an IC element, the following apply:

a. Employment

(1) New employees will not be provided access to sensitive cryptologic information until a favorably adjudicated Single-Scope Background Investigation (SSBI) and an expanded scope polygraph have been completed in accordance with all applicable requirements and standards set forth in Reference (j) and in DoD Regulation 5210.48-R (Reference (k)).

(2) To assist in determining personnel security eligibility for initial SCI access, an expanded scope polygraph examination shall be required of applicants for employment, contractor employees, and any other affiliates requiring staff-type access. A periodic counterintelligence scope polygraph will be required for assessment of eligibility for continued SCI access. Failure to consent to a polygraph examination shall result in denial or revocation of access to sensitive cryptologic information and termination of employment.

(3) All persons requiring access to sensitive cryptologic information or to spaces where sensitive cryptologic information is produced, processed, and/or stored must maintain personnel security eligibility for SCI access by a favorably adjudicated SSBI, a Single-Scope Background Investigation – Periodic Reinvestigation, or a Phased Periodic Reinvestigation, at the discretion of the DIRNSA/CHSS. Reinvestigation is required every 5 years.

b. Temporary Eligibility for SCI Access

(1) In accordance with Reference (d), applicants for NSA/CSS employment may be conditionally employed before the completion of an SSBI, but shall not be given access to sensitive cryptologic information while so employed. This procedure also extends to contractor employees, consultants, and other persons for whom the NSA/CSS has security cognizance for initial or continued access to sensitive cryptologic information. In such cases, the NSA/CSS shall determine the scope of the polygraph, as appropriate.

(2) During national emergency situations and hostilities involving U.S. personnel, the DIRNSA/CHCSS may temporarily waive the requirement for an SSBI if the Director determines in writing that such action is advisable in the national interest and is clearly consistent with the national security. This authority may be re-delegated at the discretion of the DIRNSA/CHCSS. In such cases, and wherever possible, a polygraph of appropriate scope shall be completed and favorably adjudicated prior to granting access to sensitive cryptologic information. In all cases,

priority shall be given to the completion of the SSBI, and all requirements met as set forth in Reference (j) and in Reference (k).

c. Boards of Appraisal. Reference (d) requires appointment of one or more boards of appraisal to evaluate the loyalty and suitability of persons for access to classified information, in those cases in which the DIRNSA/CHCSS determines that there is a doubt as to whether their access to that information would be clearly consistent with the national security, and delineates qualifications of the members.

d. Appeal Procedures – Denial or Revocation of Access

(1) Reference (j) establishes common appeals procedures for the denial or revocation of SCI access. Reference (i) provides guidance on the requirements to process employees for adverse action taken as a result of an adverse personnel security determination. Appeal procedures are issued pursuant to References (h) and (j).

(2) Notice to an NSA/CSS employee of the determination to revoke SCI access shall also include information regarding the intent to remove him or her from employment with the NSA/CSS for failure to meet a mandatory condition of employment; however, the notice of the proposal to remove the employee shall be a separate document.

e. Personnel Security Appeal Board. The establishment, membership, appointment, responsibilities of board members, reports and recommendations, qualifications, and security clearance requirements of board members is provided in References (d) and (i).

f. Reciprocity

(1) Office of Management and Budget Memorandum (Reference (l)) establishes security clearance reciprocity standards and procedures for the Federal Government. Reference (j) prescribes the reciprocity policy for SCI personnel security eligibility determinations.

(2) DIRNSA/CHCSS shall accept personnel security eligibility determinations for SCI granted by other agencies except those that meet one or more of the Permitted Exceptions to Reciprocity guidelines contained in Office of Management and Budget, M-06-21 (Reference (m)).

(3) A person determined ineligible after due process for SCI access will remain ineligible for a minimum of 1 year. However, IC element heads or their designees may waive this requirement in individual cases.

3. Detail or Assignment. Persons shall not be detailed or assigned to the NSA/CSS without agreement by DIRNSA/CHCSS that its security requirements have been met. Persons detailed or assigned to the NSA/CSS shall have clearance information available in appropriate security databases or certified to the NSA/CSS through official security channels. When required clearance information is not available in a security database, DIRNSA/CHCSS shall receive the

following information from the appropriate IC element head or designee prior to a person being detailed or assigned to the NSA/CSS:

a. Written confirmation of the completion and favorable adjudication of a current SSBI.

b. Written confirmation of a favorably adjudicated counterintelligence or expanded scope polygraph examination (where authorized by the cognizant IC element head) completed within the past 5 years, as set forth in Reference (k).

4. The DIRNSA/CHCSS shall reserve the right to conduct a counterintelligence scope polygraph examination of any proposed detailee or assignee to the NSA/CSS whose IC element head does not utilize the polygraph.

5. Reinvestigation Requirements. Employees who are eligible for SCI access shall be the subject of periodic reinvestigations and may also be reinvestigated if at any time there is reason to believe that they may no longer meet the established standards for access. Periodic reinvestigations shall be conducted in accordance with the standards in Reference (j).

6. Continuing Security Responsibilities. Cleared personnel who have access to sensitive cryptologic information are subject to continuous evaluation in accordance with Executive Order 13467 (Reference (n)) to ensure that they continue to meet standards of trustworthiness and reliability as set forth in Reference (j).

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CSS	Central Security Service
DIRNSA/CHSS	Director, NSA/Chief, CSS
DNI	Director of National Intelligence
DoDD	DoD Directive
DoDI	DoD Instruction
IC	Intelligence Community
NSA	National Security Agency
SCI	sensitive compartmented information
SSBI	single-scope background investigation

PART II. DEFINITIONS

These definitions are for the purpose of this Instruction only.

applicant. A person other than an employee who has received an authorized conditional offer of employment for a position that requires access to classified information.

classified information. Information that has been determined pursuant to Executive Order 12958 (Reference (o)), or any successive order; Executive Order 12951 (Reference (p)), or any successive order; or section 2011 of title 42, United States Code (Atomic Energy Act of 1954) (Reference (q)), to require protection against unauthorized disclosure.

counterintelligence scope polygraph. A personnel security interview conducted with the aid of a polygraph instrument, consisting of questions regarding espionage, sabotage, terrorism, unauthorized disclosure, secret contacts with foreign entities, and damage of U.S. Government information systems.

employee. A person employed by an agency within the intelligence community.

expanded scope polygraph. A personnel security interview conducted with the aid of a polygraph instrument, consisting of questions regarding espionage, sabotage, terrorism, unauthorized disclosure, secret contacts with foreign entities, damage of U.S. Government information systems, serious detected and undetected crimes, illegal drug involvement, and falsification of security forms.

periodic reinvestigation. Currently cleared employees are required to review, update, and resubmit his or her security clearance application for a reinvestigation. Periodic reinvestigations are routinely required every 5 years for those with SCI clearances. A periodic reinvestigation is done to ensure that an employee still meets the standards for SCI access. Reinvestigative requirements are contained in Reference (j).

reciprocity. Acceptance by one IC element head of an SCI access-eligibility determination made by another IC element head. It applies both to granting access when another IC element head has approved access, and denying access when another IC element head has denied or revoked access. Reciprocity does not include agency determinations of employment suitability. Nothing precludes IC element heads or their designees from exercising authority to grant or to deny access for reasons of operational necessity regardless of another IC element head's decision.

SCI. Highly sensitive national security information to which access is based on a strict need-to-know basis. The SCI system is a national intelligence community security program derived from intelligence sources, methods, or analytical processes, which is required to be handled exclusively within formal control systems established by the DNI. Reference (j) establishes the personnel security standards for eligibility for SCI.

sensitive cryptologic information. Classified information pertaining to or resulting from the activities and operations involved in the production of signals intelligence or the maintenance of communications security.

SSBI. An investigation standard established for employees who require SCI access which is the investigative basis for final clearance determinations. Investigative requirements are contained in References (i) and (j).