



INTELLIGENCE
COMMUNITY
DIRECTIVE
703

Protection of Classified National Intelligence, Including Sensitive Compartmented Information

A. AUTHORITY

1. The National Security Act of 1947, as amended; Executive Order (EO) 12333, as amended; EO 13526; EO 13549; EO 12829; EO 12968, as amended; 32 CFR Part 2001; 32 CFR Part 2003, 32 CFR Part 2004; and other applicable provisions of law.

2. The National Security Act of 1947, as amended provides that:

a. The Director of National Intelligence (DNI) is responsible for the protection of intelligence sources and methods from unauthorized disclosure.

b. The DNI is to establish uniform standards and procedures for granting of access to sensitive compartmented information (SCI) to any officer or employee of any agency or department of the U.S. and to employees of contractors of those agencies or departments.

3. EO 13526 provides guidance on the protection of Classified National Security Information. EO 13526 Section 6.2(b) and EO 12333, Section 1.3(b)(9) provide that the DNI, after consultation with the heads of affected departments and agencies, may issue implementing directives with respect to protecting intelligence and intelligence-related information through proper classification and declassification.

4. Pursuant to the Atomic Energy Act of 1954, as amended (42 USC 2162(e)) and 32 CFR 2001.24, the Secretary of Energy and the DNI jointly determine what information concerning the atomic energy programs of other nations is necessary to carry out the DNI's responsibilities and is to be safeguarded as classified national security information. However, automatic declassification is prohibited.

B. PURPOSE

1. This Directive establishes policy for the protection of classified national intelligence, including SCI.

2. Director of Central Intelligence Directive (DCID) 1/20P, *Security Policy Concerning Travel and Assignment of Personnel with Access to SCI*; DCID 6/1, *Security Policy for Sensitive Compartmented Information and Security Policy Manual*; Sections V and VI of DCID 6/6, *Security Controls on the Dissemination of Intelligence Information*; and IC Policy Memorandum (ICPM) 2006-700-8, *Intelligence Community Modifications to DCID 6/1 Supplement "Security Policy Manual for SCI Control Systems"* will be rescinded upon issuance of the standards required in Section G.1.a.1 of this Directive.

C. APPLICABILITY

1. This Directive applies to the Intelligence Community (IC) as defined by the National Security Act of 1947, as amended, and to such elements of any other department or agency as may be designated an element of the IC by the President, or jointly by the DNI and the head of the department or agency concerned.

2. This Directive only applies to information classified pursuant to EO 13526, Section 1.4(c).

3. This Directive also applies to the handling of SCI by any individual who receives, handles, stores, or processes SCI, including: executive departments and agencies of the U.S. Government, the Executive Office of the President, the legislative and judicial branches of the U.S. Government and all other U.S. entities as defined by EO 13526, Section 6.1(ss).

D. DEFINITIONS

1. Classified National Intelligence (CNI). National Intelligence as defined in 50 USC 401a(5), classified pursuant to EO 13526.

2. Sensitive Compartmented Information (SCI). A subset of CNI concerning or derived from intelligence sources, methods or analytical processes that is required to be protected within formal access control systems established by the DNI.

E. POLICY

1. CNI, including SCI, shall be protected from unauthorized disclosure to protect the people, mission, capabilities, and information of the IC.

2. The protection of CNI, including SCI, shall be achieved through disciplined adherence to the following:

- a. Proper application of original classification and control decisions;
- b. Proper use of derivative classification and control markings in accordance with Intelligence Community Directive (ICD) 710, *Classification Management and Control Markings System*, respective IC classification guides, IC standards, and technical specifications on machine-readable classification and control markings;
- c. Guidance issued pursuant to the declassification and downgrading authority of the DNI;
- d. National, IC, and individual IC element policies and procedures authorized by law, statute, or regulation; and
- e. Regular evaluations through self-inspection programs, and through Information Security Oversight Office (ISOO), and Office of the DNI (ODNI) reviews or reports.

3. Protection of CNI, including SCI, is also achieved through adherence to counterintelligence (CI) and security practices.

a. With regard to personnel security, persons determined eligible for and granted access to SCI in accordance with ICD 704, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information*, or other appropriate policy, incur a special and continuing security obligation to be aware of the risks associated with possible foreign intelligence operations and

possible terrorist activities directed against them in the U.S. and abroad and to be aware of the security environment in the workplace. Accordingly, these individuals shall report to their Cognizant Security Authority (CSA) as defined in IC Standard 700-1, *Glossary of Security Terms, Definitions, and Acronyms*, active or planned involvement in activities that may pose a potential threat to the protection of CNI, including SCI. This includes:

(1) Reporting to their CSA unofficial close and continuing, or suspicious contact with foreign nationals. Casual contact need not be reported;

(2) Reporting, obtaining prior approval for, and receiving appropriate defensive security briefings on unofficial foreign travel. CSAs may identify, for personnel under their purview, conditions under which prior approval is not required; and

(3) Other reporting required by the CSA.

b. With regard to physical security, all SCI must be processed, stored, used, or discussed in accordance with ICD 705, *Sensitive Compartmented Information Facilities*.

c. With regard to information assurance, all SCI must be processed, stored, and communicated in accordance with ICD 503, *Information Technology Systems Security Risk Management Certification and Accreditation*.

4. The protection measures described herein are the responsibility of any entity that receives, handles, stores, or processes CNI, including SCI, including: executive departments and agencies of the U.S. Government, the Executive Office of the President, the legislative and judicial branches of the U.S. Government, and State, local, tribal, and private sector (SLTPS) entities as described in EO 13549, *Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities*.

5. Contractors (contract employees, licensees, and grantees) may be granted access to SCI in accordance with EO 12829, *National Industrial Security Program* and pursuant to the requirements outlined in EO 13526, Section 4.1(a), ICD 704, and other applicable DNI guidance.

6. Consistent with 32 CFR 2004.22(c)(4)(ii), the DNI must concur on National Interest Determinations (NID) involving SCI.

7. Protection requirements shall be implemented in a manner that facilitates responsible sharing and appropriate dissemination of CNI, including SCI.

8. To facilitate the continued use of intelligence within and among IC elements and to provide for the timely flow to intelligence consumers, the following policy is reaffirmed. An IC element that is an authorized recipient of CNI that was created prior to the implementation of EO 13526 on 28 June 2010 and bears no restrictive control marking, may use that intelligence in CNI products and disseminate those products within executive branch departments and agencies of the U.S. Government under one of the two following conditions:

a. If the intelligence has first been sanitized by the removal of all references and inferences to intelligence sources, methods, and activities and to the identity of the producing agency, or

b. If the product is not so sanitized, but the consent of the originator has been obtained. If there is any doubt concerning reference or inference to intelligence sources, methods, and

activities, relevant intelligence documents should not be given further dissemination in this manner until the recipient has consulted with the originator.

F. IMPLEMENTATION

1. CNI, including SCI, shall be discoverable in accordance with ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*.

2. For U.S. recipients, the protection and dissemination of CNI, including SCI, is managed through the need-to-know of an appropriately cleared recipient; the proper application of classification and control markings as defined in ICD 710 and the Controlled Access Program Coordination Office's *Intelligence Community Authorized Classification and Control Markings Register and Manual*; and the use of security controls established pursuant to this directive and related standards.

3. Foreign disclosure and release of CNI, including SCI, shall occur in accordance with ICD 403, *Foreign Disclosure and Release of Classified National Intelligence*.

4. Emergency disclosure or release to U.S. recipients is a deviation from the practices referenced in Sections E.2 and E.3 and may be authorized when necessary to respond to an imminent threat to life or in defense of the homeland. An IC element head or designee may authorize the emergency disclosure of CNI, including SCI, to a U.S. individual or individuals who are not otherwise eligible for access when:

a. It is limited to the duration of the emergency and restricted to persons or entities that need the information;

b. There is insufficient time, generally less than 12 hours, to obtain approval through normal intelligence information sharing channels;

c. The information has been sanitized to the extent practical, to protect CNI, including SCI, while simultaneously facilitating the use of the information; and

d. The amount of information disclosed or released and the number of individuals to whom it is disclosed or released has been minimized.

5. Information disclosed or released under Section F.4 of this Directive shall remain classified regardless of such disclosure, release, or subsequent use by the recipient. Such disclosure or release shall be reported to the originator of the classified information within 24 hours or as soon as the emergency permits.

6. The Director of the Central Intelligence Agency (CIA) provides SCI access determinations and Sensitive Compartmented Information Facility (SCIF) accreditation for the legislative and judicial branches of the U.S. Government and for the executive branch departments and agencies, with the exception of the IC and any other department or agency who has a designated CSA or has been given the authority to grant SCI access and accredit SCIFs. The Director of CIA may further delegate this responsibility, in writing.

7. IC elements who grant access to SCI are responsible for ensuring that all those to whom they have granted access comply with all responsibilities for the protection of SCI in this Directive or any other guidance on the protection of SCI.

G. ROLES AND RESPONSIBILITIES

1. The DNI:

a. Through the National Counterintelligence Executive (NCIX), will:

(1) Issue standards no later than 120 days after the effective date of this Directive setting forth:

(a) reporting requirements for individuals with access (foreign travel and associations, media contacts, arrests, court appearances, etc.),

(b) procedures for safeguarding (indoctrination, security awareness training and education, debriefing, role of Special Security Officers, etc.),

(c) protection procedures for sharing with entities outside the IC (Federal executive, legislative, judicial branches), and with State, local, tribal and the private sector,

(d) procedures to obtain DNI concurrence on NIDs involving SCI - Foreign Ownership Control or Influence

(2) Process NID concurrence requests within 30 days of receipt.

b. Through the Assistant DNI for Partner Engagement, will address disputes arising from the sharing of CNI with foreign recipients as defined in ICD 403.

c. Through the IC Information Sharing Executive, consistent with ICD 501, will address disputes arising from the sharing of CNI with U.S. recipients.

d. Through the IC Chief Information Officer, will:

(1) Issue standards and technical specifications to implement EO 13526 within the IC Information Technology Environment (IC ITE) covering the topics of:

(a) classification and declassification of CNI,

(b) providing access to CNI in the IC ITE, and

(c) dissemination of CNI in the IC ITE, both in its final form and in the form when initially gathered.

(2) Establish integrated defense and security controls, in accordance with ICD 502, *Defense of the Intelligence Community Information Environment*, and ICD 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification, and Accreditation*, including information technology standards, in order to protect and defend CNI, including SCI.

(3) Coordinate with the Department of Energy (DOE) on the classification, declassification, and security of Atomic Energy Act information in intelligence products and systems.

2. Heads of IC elements shall:

a. Ensure that access to SCI by each employee, as defined in EO 12333, Section 3.5(d) is in accordance with EO 12968, Section 1.2(c).

- b. Ensure that the intended recipients agree, by signing approved SCI or other non-disclosure agreements, as appropriate, to follow prescribed protection, handling, accountability, storage, dissemination, and destruction requirements.
- c. Designate a CSA for their element to serve as the IC element authority for all aspects of security program management, or if appropriate utilize departmental resources, in accordance with ICD 700, *Protection of National Intelligence*.
- d. Submit requests for NID concurrences to the Office of the NCIX, in accordance with 32 CFR 2004.5(d) and 2004.22(c), prior to giving contractors access to SCI for all new contract requirements, including pre-contract activities and existing contracts consistent with Section E.6 of this Directive.
- e. Coordinate with the DOE on the classification, declassification, and security of Atomic Energy Act information in intelligence products and systems.


3. CSAs may:

- a. Designate additional personnel, as necessary, to implement this Directive.
- b. Develop and promulgate guidance for their IC element and any additional parties for whom they are responsible, consistent with this Directive, for additional requirements related to the protection of CNI, including SCI.

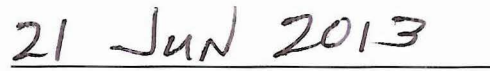
4. Individuals with authorized access to SCI shall:

- a. Have received a favorable determination for access to SCI by an appropriate authority prior to receiving access.
- b. Comply with all provisions of signed non-disclosure agreements as required by EO 13526, Section 4.1 and 32 CFR 2001.80.
- c. Comply with all reporting requirements and any additional guidance as may be issued by the responsible CSA.
- d. Maintain awareness of CI and security risks associated with possible foreign intelligence activities and possible terrorist activities directed against cleared personnel in the U.S. and abroad.

H. EFFECTIVE DATE: This Directive becomes effective on the date of signature.



Director of National Intelligence



Date