

Controlled Access Programs

A. **AUTHORITY:** The National Security Act of 1947, as amended; Executive Order (EO) 12333, as amended; EO 13526; EO 12968, as amended; and other applicable provisions of law.

B. **PURPOSE**

1. This Directive defines the policy, framework, and process for ensuring effective oversight and management of Intelligence Community (IC) special access programs pursuant to EO 13526, Section 4.3, referred to within the IC as Controlled Access Programs (CAP).

2. This Directive also establishes programmatic security practices and procedures for accessing and safeguarding CAP information.

3. This Directive rescinds Director of Central Intelligence Directive 6/11, *Controlled Access Program Oversight Committee* and Intelligence Community Policy Memorandum 2006-700-10, *Intelligence Community Update to DCID 6/11*.

C. **APPLICABILITY**

1. This Directive applies to the 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 Director of National Intelligence (DNI) and the head of the department or agency concerned.

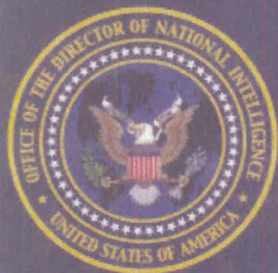
2. This Directive applies to CAPs created under the DNI's authority, which includes Sensitive Compartmented Information (SCI) and non-SCI CAPs. Pursuant to EO 13526, Section 4.3, the DNI has authority over CAPs pertaining to intelligence sources, methods, and activities but does not have authority over military operational, strategic, or tactical programs.

3. This Directive does not apply to special access programs created pursuant to EO 13526, Section 4.3 by the Secretaries of State, Defense, Energy, or Homeland Security or the Attorney General or their principal deputies. Nor does this Directive apply to special access programs under the purview of the National Security Council, such as covert action.

D. **DEFINITIONS**

1. **Controlled Access Program (CAP):** Within the Intelligence Community, "Controlled Access Program" refers to a top-level control system (such as SI, TK, HCS) and any compartment or sub-compartment under a control system. Unless otherwise indicated, references to CAPs in this document refer to all levels within the CAP.

2. **Control System:** The top-most level within the CAP structure, under which its compartments and sub-compartments reside.



3. CAP Program Manager: The CAP Program Manager is responsible for administering a CAP on behalf of the DNI. A CAP Program Manager may be an IC element head or designated senior representative. The authorities and responsibilities of the CAP Program Manager are set forth in this Directive.

4. Compartment or Sub-compartment: The only levels of subordinate structure within a control system.

5. Control Officer: A government employee or contractor who has been authorized by the CAP Program Manager to administer and enforce policy and procedures that govern the execution of a control system, compartment, or sub-compartment.

6. Non-SCI CAP: CAPs that are not bound to SCI-accredited standards (for example, a CAP that is executed at the SECRET level) and typically permit the use of people, facilities, computers, and networks that are not SCI.

7. Portfolio: A methodology used to identify a group of individuals focused on a specific topic or region, which requires access to a common set of associated controlled access programs to support integration, unity of effort, and timely collaboration.

8. Sensitive Compartmented Information: As defined in ICD 703, *Protection of Classified National Intelligence, Including Sensitive Compartmented Information*, a subset of classified national intelligence 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.

9. Special Access Program: A program established, under EO 13526, Section 4.3, for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information classified at the same classification level.

10. Unacknowledged CAPs: Those CAPs with protective controls that ensure the existence of the program is not acknowledged, affirmed, or made known to any person not authorized for such information.

E. POLICY

1. Only the DNI and Principal Deputy DNI (PDDNI) have the authority to create, validate, substantially modify¹, or terminate CAPs.

a. The DNI delegates the authority to create, substantially modify, or terminate compartments and sub-compartments subordinate to an established control system through the head of the IC element to the CAP Program Managers.

b. The creation, substantial modification, or termination of a compartment or sub-compartment must be validated by the Senior Review Group (SRG). New compartments and

¹ For the purpose of this Directive, *substantially modify* refers to any proposed change that causes the nature of that control system, compartment, or sub-compartment to differ from what is already approved, such as changing the status of a CAP from unacknowledged to acknowledged or changing the purpose or structure of a control system.

sub-compartments not validated consistent with Section F.2.a of this Directive will be terminated.

2. In accordance with EO 13526, Section 4.3, CAPs shall be used to protect the nation's most sensitive and critical intelligence sources, methods, and activities and shall be established or validated only upon a specific finding that:

a. The vulnerability of, or threat to, specific information is exceptional and the normal criteria for determining eligibility for access to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure; or

b. The CAP is required by statute.

3. Minimum and maximum protection requirements for control systems, including their compartments and sub-compartments, shall reflect the need to both safeguard and allow appropriate access to this exceptionally sensitive information.

a. Only the DNI or PDDNI may establish minimum and maximum protection requirements for a CAP. The CAP Program Manager shall determine the appropriate level of protections for their CAP, within the minimum and maximum protections set by the DNI or PDDNI.

b. Information contained within a CAP shall be protected consistent with the measures described for SCI in ICD 703, regardless of the classification level of the CAP. Only the DNI or PDDNI may approve alternative protections.

c. Any exemptions from these protection requirements provided in accordance with Section E.10 of this Directive shall be reviewed and validated annually, consistent with Section E.5 of this Directive.

4. Access to a control system does not automatically include access to all subordinate compartments and sub-compartments.

5. All CAPs shall be reviewed and revalidated by the DNI or PDDNI at least annually based on the criteria in EO 13526, Section 4.3. CAPs not revalidated shall be terminated and the protected information shall be decompartmented or protected by a validated CAP.

6. Responses to CAP access requests, in the form of either an approval or a denial with justification, shall be provided within five business days from the request.

7. The indoctrination briefing, non-disclosure agreement, and any other administrative information necessary for indoctrination into a CAP shall be stored in a manner that permits appropriately cleared individuals to be indoctrinated within two business days of the CAP Program Manager or designee authorizing access.

8. Sanitization, tearlines, and other write-for-release principles described in ICD 208, *Write for Maximum Utility*, apply to intelligence derived from CAP information.

9. Intelligence and intelligence-related information within CAPs shall be discoverable or exempted from discovery consistent with the processes outlined in ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community* and its associated Policy Guidance.

10. Exemptions from any provision of this Directive shall be approved only by the DNI or PDDNI.

F. IMPLEMENTATION

1. CAP Management, Oversight, and Administration: CAP management and oversight shall be accomplished via the Controlled Access Program Oversight Committee (CAPOC), SRG, and Controlled Access Program Management (CAP Management). CAP administration shall be accomplished via the CAP Program Managers.

a. The CAPOC Chair is responsible for CAP oversight within the IC. CAP oversight includes ensuring the creation and validation of only those CAPs necessary to protect intelligence sources, methods, and activities. The CAPOC Chair is also responsible for making recommendations to the DNI or PDDNI for the creation, validation, substantial modification, or termination of control systems. These recommendations are based on SRG review.

(1) The CAPOC is not a standing body but convenes as required, either in person or virtually, to address specific issues and, as appropriate, validate the SRG recommendations prior to submission to the DNI or PDDNI.

(2) CAPOC membership depends on the issue the CAPOC is addressing and may include:

(i) The head or deputy head of the IC element for CAPOC discussions on CAPs administered by their IC elements.

(ii) The Deputy Secretary of Defense or designee for discussions on CAPs administered by IC elements in the Department of Defense (DoD).

(iii) Others, as determined by the CAPOC Chair, in consultation with the affected CAP Program Manager.

b. The CAP management responsibilities of the SRG include reviewing control systems and their compartments and sub-compartments for creation, validation, substantial modification, or termination; audits and evaluations consistent with EO 13526, Sections 4.3 and 5.4(d); and ensuring there is no conflict or unnecessary duplication between CAPs and other government programs.

(1) Members of the SRG and CAP Management shall have access to all IC control systems, compartments, and sub-compartments, unless the CAPOC Chair determines otherwise. Knowledge of information within these control systems, compartments, and sub-compartments will be limited to what is necessary to perform the functions described in this Directive.

(2) SRG membership shall include principals or deputies from applicable ODNI components and senior representatives from IC elements that administer a CAP. Specific membership will be established in the SRG Charter.

c. CAP Program Managers administer CAPs on behalf of the DNI, consistent with Section G.6.a of this Directive. Administration includes: setting protection requirements consistent with Section E.3; making need-to-know determinations for individuals requesting access to a CAP; designating, approving, and training control officers; coordinating on decisions regarding inclusion of compartments and sub-compartments in portfolios; and general

coordination or consultation with the SRG to ensure informed oversight and management. CAP Program Manager responsibilities may be further delegated.

d. CAP Management provides expertise, staffing, and secretariat support to the CAPOC and the SRG. CAP support includes working with CAP Program Managers from IC elements to ensure effective and efficient implementation of this Directive.

e. Members of the SRG and CAP Management shall complete a favorably adjudicated Counterintelligence-Scope polygraph examination, at a periodicity determined by the DNI or designee. Members shall be fully cleared, consistent with ICD 704, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartment Information and Other Controlled Access Program Information*.

2. Procedures:

a. New compartments or sub-compartments must be submitted to the DNI or designee for validation at least 15 business days prior to creation; in cases in which this is not feasible, they should be validated no later than five business days after creation, consistent with Section E.1.b of this Directive.

b. CAP accesses shall be included in Scattered Castles or successor systems.

(1) Only the DNI or PDDNI may approve exemptions to this requirement.

(2) To ensure accuracy, individual accesses in Scattered Castles or successor systems consistent with ICPG 704.5, *Intelligence Community Personnel Security Database Scattered Castles*, shall be updated within two business days of a change in access.

(3) Scattered Castles, or successor systems, is the authoritative repository for verifying and validating an individual's CAP accesses.

c. When mission needs require, consistent with the portfolio process, portfolios that contain multiple CAPs may be created with the approval of the CAPOC Chair, based upon the recommendation of the SRG and in coordination with the affected CAP Program Managers, to enhance timely collaboration. The PDDNI is the IC's approval authority for Joint DoD and IC portfolios.

d. The process and timeline described in ICPG 501.2, *Sensitive Review Board and Information Sharing Dispute Resolution Process* shall be used for resolving disputes related to the denial of access to a CAP or the inclusion of a CAP in a portfolio. This process includes appeal to the DNI, as necessary.

(1) The ICPG 501.2 process applies only if the denial is based on the individual's need-to-know determination.

(2) If the denial is based on a clearance or adjudication determination made in accordance with ICD 704 adjudication criteria, the appeals process in ICPG 704.3, *Denial or Revocation of Access to Sensitive Compartmented Information, other Controlled Access Program Information, and Appeals Processes* applies.

e. Requests for exemptions pursuant to Section E.10 shall be submitted with justification to the SRG for review. Final recommendations to the DNI or PDDNI shall be made

by the CAPOC Chair. Any exemptions approved will be reviewed for continuation or termination during the annual review described in Section E.5.

(1) An exemption may be requested for a group of compartments or sub-compartments related to a single region or topic.

(2) If mission needs require an expedited exemption process, such as for a time-sensitive control system or subordinate compartment or sub-compartment, a justification for expediting must be provided with the initial submission. Expedited exemption requests will be processed in accordance with this justification.

(3) Exemptions to the maximum requirements defined in Section F.3 must be submitted within the first year after signature of this Directive. Any exemptions not requested or approved within the first year will no longer be permitted.

3. Protection Requirements: Minimum and maximum protection requirements are established by the DNI and PDDNI. Only the DNI or PDDNI may authorize any exemptions to the personnel, information, or physical security protections outlined below. Protections shall include the following:

a. Personnel security: Prior to gaining access to a CAP and as a condition for access, all personnel must have a favorably adjudicated TOP SECRET clearance and be approved for SCI access in accordance with ICD 704; be appropriately indoctrinated into the program; and comply with any polygraph requirements established by the CAP Program Manager for access to the CAP information in question.

b. Information Technology Security:

(1) Any separation of CAP information shall be achieved through logical construct rather than by physical separation, to the greatest extent possible, and in accordance with applicable law and policy requirements.

(2) CAP information shall be identified as such in metadata tags defined in IC Technical Specifications established by the IC CIO in accordance with Section G.4.a of ICD 710, *Classification Management and Control Markings System*.

(3) Consistent with existing information technology security policy and guidance (i.e., ICD 503, *Intelligence Community Information Technology Systems Security Risk Management*, Committee on National Security Systems Instruction 1253, and the Intelligence Overlay), all systems processing CAP information shall ensure that adequate security controls are applied.

c. Physical Security: In order to prevent access by those not indoctrinated into a program, CAP information shall be physically protected as follows:

(1) ICD 705, *Sensitive Compartmented Information Facilities (SCIFs)*, sets uniform security requirements for the protection of SCI material. Any SCIF accredited in accordance with the requirements defined in ICD 705 and subsequent guidance also provides the minimum level of protection for CAP information.

(2) A CAP Program Manager may request an exemption consistent with Section E.10 of this Directive, on the grounds that the uniform security requirements in ICD 705 do not

provide sufficient protection. If the exemption is approved, a SCIF within an accredited SCIF may be used consistent with the exemption.

(i) Compartmented areas allow for CAP information to be viewed, processed, stored, and discussed in an accredited SCIF with additional standardized protections such as those described in Chapter 2, Section C of the *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities (v1.2)*.

(ii) The establishment of a SCIF within a SCIF must be explicitly authorized by the DNI or PDDNI through the exemption request.

d. DNI or PDDNI approval is required for the use of billet lists (which control access to a CAP in terms of a defined number of people) and bigot lists (by-name or -position access). The billet number and by-name access must be justified to and approved by the SRG at the creation of a CAP and revalidated during the annual review required in Section E.5 of this Directive. During the creation or re-validation, the SRG will consult with affected IC elements prior to approving the use or continued use of billets or bigots.

(1) CAP Program Managers currently using billets or bigots as a protection for the information in the CAP they administer must provide a justification to the SRG for the current bigots and number of billets allotted to each IC element or other non-IC organization during the next annual review.

(2) CAP Program Managers have the authority to temporarily expand or reduce approved billet lists as operational and intelligence needs dictate, with notification to the SRG.

e. Emergency disclosure and release of CAP information shall be carried out consistent with ICD 703, with regard to U.S. entities, and ICPG 403.3, *Criteria and Conditions for Emergency Foreign Disclosure and Release*, with regard to disclosure or release to foreign entities.

G. ROLES AND RESPONSIBILITIES

1. The DNI or PDDNI will:

- a. Designate a senior ODNI official as the Chair of the CAPOC;
- b. Create, validate, substantially modify, or terminate control systems, after consideration of CAPOC Chair recommendations;
- c. Create, validate, substantially modify, or terminate compartments and sub-compartments under an established control system, unless delegated;
- d. Establish minimum and maximum protection requirements for CAP information, including personnel, physical, and information security requirements; and
- e. Approve exemptions to this Directive.

2. The CAPOC Chair shall:

- a. Designate a senior ODNI official as the Chair of the SRG;
- b. Review SRG findings, in coordination with the CAPOC as appropriate, and provide recommendations at least annually to the DNI to create, validate, substantially modify, or

terminate control systems, including their compartments and sub-compartments, unless delegated;

- c. Oversee the management of CAPs and their compartments and sub-compartments;
- d. Approve IC CAP portfolios;
- e. Direct CAP audits and performance evaluations as required, consistent with EO 13526, Sections 4.3 and 5.4(d);
- f. Establish a charter for the SRG that describes its roles and responsibilities, consistent with this Directive; and
- g. Issue IC Standards and procedures, as appropriate, for CAP processes, consistent with ICPG 101.2, *Intelligence Community Standards*.

3. The SRG Chair shall:

- a. Review at least annually the creation, validation, substantial modification, or termination of control systems, including their compartments or sub-compartments;
- b. Validate compartments and sub-compartments, in coordination with the CAP Program Managers;
- c. Assist the CAPOC Chair in providing oversight and evaluation of control systems and their compartments and sub-compartments; and
- d. Provide congressional briefings and notifications on CAPs, as appropriate, in accordance with ICD 112, *Congressional Notification*, and in coordination with the affected CAP Program Manager.

4. The Director of CAP Management shall:

- a. Maintain a list of all control systems, including compartments and sub-compartments;
- b. Ensure that all authorized control systems, their compartments, and sub-compartments are incorporated into Scattered Castles;
- c. Ensure that control system names, abbreviations, and cover sheets, including compartment or sub-compartment names, do not conflict with each other;
- d. Create a virtual space that will allow for CAP indoctrination information to be accessible at each IC element. Any such space must have appropriate access controls. Use of this space is not required if indoctrination information is otherwise accessible at each element;
- e. Coordinate annual program reviews of control systems and their compartments and sub-compartments in support of the SRG and CAPOC;
- f. Serve as the Community focal point for issues and processes concerning the management and administration of control systems, compartments, and sub-compartments;
- g. Notify the SRG Chair of a request by the CAP Program Managers to validate the creation, substantial modification, or termination of compartments or sub-compartments; and
- h. Support the CAPOC and SRG Chairs in the development of IC Standards for CAPs.

5. Heads of IC elements shall designate a point of contact for all CAP administration-related issues within that element. This person may be the person responsible for the Sensitive Review Board as discussed in ICD 501.

6. Heads of IC elements responsible for administering CAPs shall:

a. Designate a program manager for each CAP they administer who is responsible for:

(1) Being the point of contact for programmatic recommendations regarding that CAP;

(2) Establishing and implementing the protection requirements for the CAP, consistent with Sections E.3 and F.3 of this Directive, and notifying the SRG of any waiver to the polygraph requirement set in accordance with Section F.3.a;

(3) Ensuring that the creation, validation, substantial modification, and termination of control systems, compartments, and sub-compartments is consistent with this Directive and any subsequent IC policy and standards;

(4) Requesting validation from the SRG through CAP Management 15 business days prior to creating compartments or sub-compartments. If operational requirements do not allow a request for validation within this timeframe, the request should be made as soon as possible, but no later than five business days after the creation of the compartment or sub-compartment;

(5) Notifying the SRG through CAP Management at least 15 business days prior of the intent to substantially modify or terminate compartments or sub-compartments. The notification shall include an updated description of the compartment or sub-compartment;

(6) Conducting and submitting annual reviews of all control systems to the CAPOC Chair, including compartments and sub-compartments, pursuant to CAPOC guidance;

(7) Managing access lists for control systems, compartments, and sub-compartments, including billeted and bigoted programs, and coordinating with CAP Management to ensure inclusion in Scattered Castles;

(8) Designating, training, and delegating authorities to a Control Officer at each IC element for indoctrination and debriefing of CAPs, insofar as the head of the IC element does not make indoctrinations locally available through the use of the virtual space created pursuant to Section G.4.e;

(9) Supporting the SRG Chair in the development of congressional briefings and notifications pursuant to Section G.3.d;

(10) Coordinating with CAP Management on the annual review and validation described in Section E.5;

(11) Annually certifying to the CAPOC Chair that CAP oversight mechanisms and processes are consistent with this Directive;

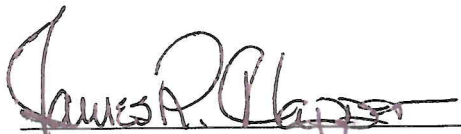
(12) Approving CAP access requests or providing justification of why a request is denied, within five business days from the request; and

(13) Reviewing and responding to proposed portfolios affecting CAPs for which they are responsible within 14 days of receipt of the proposed portfolio. CAP Management may consider extensions on a case-by-case basis.

b. Designating a representative to the SRG responsible for representing the element's position with regard to CAP management and oversight; and

c. Ensuring proper reporting of adverse information on personnel with access to a CAP to the Cognizant Security Office.

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



Director of National Intelligence

17 OCT 2015
Date