INTELLIGENCE COMMUNITY DIRECTIVE

906

Controlled Access Programs

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

B. PURPOSE:

1. This Intelligence Community Directive (ICD) establishes the oversight and management of Intelligence Community (IC) special access programs pursuant to EO 13526, Section 4.3, or any successor document, referred to within the IC as Controlled Access Programs (CAPs).

2. This ICD supersedes ICD 906, *Controlled Access Programs*, signed 17 October 2015.

C. APPLICABILITY

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

2. This Directive applies to CAPs established under the DNI's authority, which includes Sensitive Compartmented Information (SCI) and non-SCI CAPs. The DNI may establish CAPs pertaining to intelligence sources, methods, and activities but does not have authority to establish military operational, strategic, or tactical programs.

3. This Directive does not apply to special access programs established pursuant to EO 13526, Section 4.3, or any successor document by the Secretaries of State, Defense, Energy, or Homeland Security or by 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. POLICY

1. There shall be established CAPs to protect extraordinarily sensitive national security operations, capabilities, and intelligence activities. In accordance with EO 13526 or any successor document, the establishment of CAPs shall be kept to an absolute minimum, and only be used to protect the nation's most sensitive and critical intelligence sources, methods, and activities. The consideration of CAPs shall also include whether or not the establishment of a CAP would restrict access to information in a manner that may reasonably have negative planning or operational effects. CAPs, including unacknowledged

CAPs, shall be established only if required by statute, or if the DNI determines the following criteria are met and memorialized in a detailed justification statement:

a. The vulnerability of, or threat to, the specific information is exceptional, due to the sensitivity of the information and consequences of loss, compromise, or unauthorized disclosure, and necessitates additional safeguarding procedures beyond those required for collateral classified national security information;

b. The normal criteria for determining eligibility for access to collateral classified national security information are insufficient to protect such information from loss, compromise, or unauthorized disclosure, and access requires additional personnel security vetting procedures, a non-disclosure agreement, and a defined access list; and

c. Consideration has been given as to whether there are no other means to limit access to the information requiring protection or, if there are other means, using such means would result in unacceptable risk.

2. Only the DNI or the Principal Deputy Director of National Intelligence (PDDNI) have the authority to establish, validate, modify, or terminate CAPs. For the purpose of this Directive, CAPs are defined as a top-level control system (such as Special Intelligence, Talent Keyhole, Human Intelligence Control System), and any compartment or sub-compartment under a control system within the IC. Unless otherwise indicated, references to CAPs in this Directive refer to all levels within the CAP.

a. A Control System is the top-most level within the CAP structure, under which its compartments and sub-compartments reside. Compartments and sub-compartments are the only levels of subordinate structure within a control system. There shall not be any levels beyond the sub-compartment levels, unless the DNI or PDDNI determine or approve otherwise.

b. For any additional caveats or restrictions outside of CAPs, approval must be granted by the DNI or PDDNI.

c. For the purpose of this Directive, a modification is any significant change to the control system, compartment, or sub-compartment (for example, its size, scope, or accesses).

3. Consistent with Section D.2 of this Directive, unacknowledged CAPs may be established only where knowledge of the existence of a program would reveal aspects of its protected information, and when there is no other means to protect information about programs at the collateral classification level, or when required by statute. Unacknowledged CAPs may be established only with the approval of the DNI or PDDNI.

4. Only the DNI or PDDNI may establish minimum and maximum access and protection requirements for a CAP, and all levels associated with CAPs. All information held at the control system, compartment, or sub-compartment level shall be protected consistent with the measures described in ICD 703, *Protection of Classified National Intelligence Including Sensitive Compartmented Information*, and other applicable guidance. Protections shall balance both the need to safeguard CAP information and the need to ensure CAP information can be accessed and used in support of the IC's mission. Only the DNI or PDDNI may approve alternative protections.

5. Intelligence and intelligence-related information within all 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 implementing guidance. Any exemption from this requirement shall be approved only by the DNI or PDDNI, and reviewed and validated at least annually.

6. All CAPs shall be recorded, and individual accesses to those CAPs shall be included, in the authoritative repository, Scattered Castles, or its successor system, for verifying and validating all CAP accesses, consistent with Intelligence Community Policy Guidance (ICPG) 704.5, *Intelligence Community Personnel Security Database Scattered Castles*. Any exemption from this requirement shall be approved only by the DNI or PDDNI, and reviewed and validated at least annually.

a. Cleared personnel with a justified need-to-know shall generally be eligible for CAP access unless additional restrictions have been authorized by the DNI or PDDNI. In circumstances where additional access limitations may be required, accesses may be further limited by billets (a number of accesses to compartments and sub-compartments) or by name or position (BYNOP). The use of billet or BYNOP restrictions requires approval by the DNI or PDDNI, and shall be reviewed at least annually.

7. To provide oversight and accountability, there shall be a CAP Oversight Committee (CAPOC), which the PDDNI or the PDDNI's designee shall chair. The CAPOC Chair shall be responsible for CAP oversight and the management of CAPs, to include all unacknowledged CAPs, necessary to protect intelligence sources, methods, and activities, and any exemptions that may be requested. The members of the CAPOC shall be deputies of IC elements, as determined by the DNI or PDDNI. The CAPOC Chair shall:

a. Ensure members of the CAPOC have access to all IC CAPs, unless the CAPOC Chair determines otherwise, and have knowledge of information within these CAPs as needed to perform the functions described in this Directive;

b. Oversee the Senior Review Group (SRG) in its role in the oversight and management of CAPs;

c. Review SRG recommendations, in coordination with the CAPOC, as appropriate, and provide recommendations at least annually to the DNI to establish, validate, modify, or terminate CAPs;

d. Maintain a charter, in accordance with ODNI Memorandum ES 2021-01996, *Intelligence Community Charters*, 23 February 2022, for the SRG that describes its membership and roles and responsibilities, consistent with this Directive; and

e. Approve CAP portfolios to provide for a group of individuals to have access to a common set of associated CAPs to support integration, unity of effort, and timely collaboration. For Joint Department of Defense and IC portfolios, the PDDNI is the IC's approval authority.

8. There shall be an SRG with CAP management responsibilities including reviewing and making recommendations to the CAPOC on all CAPs, including unacknowledged CAPs. This includes the establishment, validation, modification, or termination of CAPs, as well as any

exemptions from any provision of this Directive. There shall be an SRG Chair designated by the CAPOC Chair to serve in this role. SRG membership shall be comprised of senior officials designated by the heads of IC elements as determined by the PDDNI, including the heads of IC elements that administer a CAP, ODNI offices designated by the PDDNI, and any others as determined by the DNI or PDDNI. The SRG Chair shall:

a. Ensure members of the SRG have the appropriate access to CAPs, unless the SRG Chair determines otherwise, and have knowledge of information within these CAPs as needed to perform the functions described in this Directive;

b. Develop a charter, in accordance with ODNI Memorandum ES 2021-01996, *Intelligence Community Charters*, 23 February 2022, for the SRG signed by the DNI or PDDNI that describes its roles and responsibilities consistent with this Directive;

c. Ensure that CAPs are reviewed periodically to deconflict any potential conflicts or unnecessary duplication between CAPs and other government programs, consistent with EO 13526 or any successor document;

d. Review at least annually the establishment, validation, modification, or termination of CAPs, to include those that are unacknowledged;

e. Provide recommendations to the CAPOC Chair on oversight and evaluation of CAPs;

f. Provide analysis and reports on CAPs, consistent with EO 13526 or any successor document, and as needed to ensure CAPs are continuously in compliance with this Directive;

g. Review and provide recommendations on requests to use billeted or BYNOP restrictions;

h. Recommend to the CAPOC Chair the establishment of CAP portfolios;

i. Review and manage IC element requests to modify or terminate CAPs consistent with this Directive; and

j. Make recommendations to the DNI or PDDNI regarding the establishment of CAPs, to include unacknowledged CAPs, and any exemptions that may be requested, or any other necessary decisions or escalations.

9. The Director of the ODNI Controlled Access Program Central Office (CAPCO) is the accountable official responsible for the implementation of this policy and for issuing IC Standards (ICS), consistent with ICPG 101.2, *Intelligence Community Standards,* and procedures, as appropriate, for CAP processes. The ODNI CAPCO shall:

a. Serve as the central point of contact for all CAP requirements in this Directive for the IC, and provide any guidance necessary to manage CAPs, accesses, and exemptions;

b. Manage a CAP Registry that maintains a list of all control systems, including all compartments and sub-compartments. ODNI CAPCO shall also ensure deconfliction or all other programs, and manage all compartment and sub compartment names, codenames, and any other pertinent information;

c. Be responsible for the coordination of CAP-related engagements, to include, but not limited to, congressional briefings, requests from the Information Security Oversight Office, and the National Security Council; and

d. Ensure all records pertaining to CAPs are maintained, and ensure that at least one records official is cleared to all CAP information in accordance with EO 13526.

10. IC elements shall administer CAP responsibilities on behalf of the DNI. IC elements shall submit requests to establish, modify, or terminate compartments and sub-compartments subordinate to established control systems for DNI or PDDNI approval. To effectively administer CAPs, IC elements shall:

a. Designate a senior CAP official (hereinafter, CAP Program Manager) to be responsible for administering the CAPs on behalf of the DNI or PDDNI consistent with EO 13526. The CAP Program Manager shall be authorized to administer CAP management, oversight, and governance;

b. Submit justification requests to the ODNI CAPCO for CAP establishments, modifications, or terminations of all CAPs, to also include unacknowledged CAPs, requests for exemptions, or any other CAP-related matters. Any new CAPs not submitted, and approved, will be terminated;

c. Implement the level of protections for the CAPs being administered within the minimum and maximum protections set by the DNI or PDDNI. Protections shall reflect both the need to safeguard CAP information and the need to enable CAP information to be used in support of the IC's mission;

d. Maintain an internal tracking mechanism for the CAPs being administered that documents the name, general information, and any unique information about the CAP, under requirements set by the DNI or PDDNI;

e. Submit requested information to ODNI CAPCO to support each CAP's annual review so they can be thoroughly reviewed, justified, and submitted for re-validation by the DNI or PDDNI based on the criteria in EO 13526. CAPs not re-validated shall be terminated and the protected information shall be de-compartmented or protected by a validated CAP;

(1) For unacknowledged CAPs, IC elements shall include in their annual review submission, a justification for why each such CAP still meets the requirements to be unacknowledged.

(2) For any exemptions from requirements established in this Directive, IC elements shall include in their annual review submission, a justification for why each exemption is still needed.

(3) IC elements shall evaluate on an ongoing basis, at least quarterly, whether CAPs should continue to exist. IC elements shall submit to the DNI or PDDNI any recommendations to terminate CAPs.

f. Ensure accesses to CAPs are managed and facilitated by designated personnel within each IC element, consistent with Section D.6 of this Directive; and

g. Ensure all records pertaining to CAPs are maintained, and ensure that at least one records official is cleared to all CAP information in accordance with EO 13526.

11. Only the DNI or PDDNI may approve exemptions from any provision of this Directive.

E. ROLES AND RESPONSIBILITIES

1. The DNI or PDDNI shall:

a. Establish, validate, modify, or terminate control systems, and their compartments and sub-compartments, after consideration of CAPOC Chair recommendations;

b. Establish unacknowledged CAPs and/or approve non-discoverability of CAPs if a compelling case can be made that any agreed upon approach to discoverability would reveal a capability, a decision, or a fragile source, and the information contained in the compartment is so narrowly tailored, it is unlikely to be of use to officers who do not already have access to the compartment;

c. Establish minimum and maximum access and protection requirements for all CAPs; and

d. Approve all exemptions from this Directive, and review and approve annually.

2. The CAPOC Chair shall:

a. Provide CAP oversight and recommendations to the DNI and PDDNI for the establishment of CAPs, to include all unacknowledged CAPs, and any exemptions that may be requested;

b. Ensure members of the CAPOC have relevant accesses to CAPs, unless the CAPOC Chair determines otherwise, and have knowledge of information within these CAPs as needed to perform the functions described in this Directive;

c. Develop an SRG charter, signed by the DNI or PDDNI, describing its membership and roles and responsibilities;

d. Oversee the SRG and review SRG recommendations, in coordination with the CAPOC, as appropriate, and review and provide recommendations to the DNI at least annually to establish, validate, modify, or terminate CAPs;

e. Oversee IC elements' management of control systems and their compartments and sub-compartments; and

f. Approve IC CAP portfolios.

3. The SRG Chair shall:

a. Develop a charter, in accordance with ODNI Memorandum ES 2021-01996, *Intelligence Community Charters*, 23 February 2022, for the SRG that describes its roles and responsibilities consistent with this Directive;

b. Review and manage IC element requests to modify or terminate CAPs consistent with this Directive;

c. Conduct reviews at least annually to make recommendations for the establishment, validation, modification, or termination of CAPs, including unacknowledged CAPs;

d. Provide recommendations to the CAPOC Chair on oversight and evaluation of CAPs;

e. Provide analysis and reports on CAPs as needed to ensure compliance, consistent with EO 13526, and as needed to ensure CAPs are continuously in compliance with this Directive;

f. Ensure members of the SRG have relevant accesses to CAPs, unless the SRG Chair determines otherwise, and have knowledge of information within these CAPs as needed to perform the functions described in this Directive;

g. Ensure CAPs are reviewed periodically to deconflict any potential conflicts or unnecessary duplication between CAPs and other government programs;

h. Review and provide recommendations on access restrictions for billeted and BYNOP requirements, to include annual reviews;

i. Recommend to the CAPOC Chair the establishment of CAP portfolios; and

j. Provide recommendations to the DNI or PDDNI regarding the establishment of CAPs, including unacknowledged CAPs, and any exemptions being requested, or any other decisions or escalations.

4. The Director of ODNI CAPCO shall:

a. Serve as a central point of contact for all CAP requirements in this Directive for the IC;

b. Provide guidance to the IC as necessary to manage CAPs, accesses, and exemptions;

c. Maintain the CAP Registry, a list of all control systems, including all compartments and sub-compartments;

d. Deconflict all IC CAPs or all other programs to ensure deconfliction and management of CAPs, and manage all compartment and sub compartment names, codenames, and any other pertinent information;

e. Issue IC Standards and procedures, as appropriate, for CAP processes, consistent with ICPG 101.2, *Intelligence Community Standards*;

f. Be responsible for the coordination of CAP-related engagements, to include, but not limited to, congressional briefings, requests from the Information Security Oversight Office, and the National Security Council; and

g. Ensure all records pertaining to CAPs are maintained, and that at least one records official is cleared to all CAPs.

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

a. Designate a CAP Program Manager to be responsible for administering CAP responsibilities on behalf of the DNI or PDDNI;

b. Submit requests to establish, modify, or terminate compartments and sub-compartments subordinate to established control systems for DNI or PDDNI approval;

c. Submit justification requests for CAP establishments, modifications, or terminations of all CAPs, to also include unacknowledged CAPs, requests for exemptions, or any other CAP-related matters, to the DNI or PDDNI;

d. Ensure the balancing of both the need to safeguard CAP information and the need to enable CAP information to be used in support of the IC's mission;

e. Determine and implement appropriate levels of protections for the CAPs being administered within the minimum and maximum protections set by the DNI or PDDNI;

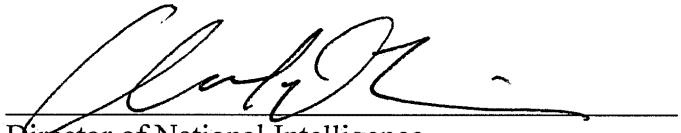
f. Maintain an internal tracking mechanism for the CAPs being administered that documents the name, general information, and any unique information about the CAP, as set by the DNI or PDDNI;

g. Submit requested information to ODNI CAPCO to support each CAP's annual review so they can be thoroughly reviewed, justified, and submitted for re-validation by the DNI or PDDNI;

h. Ensure CAP accesses are managed and facilitated by designated personnel within each IC element; and

i. Ensure all records pertaining to CAPs are maintained, and that at least one records official is cleared to all CAP information.

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



Director of National Intelligence

December 17, 2024

Date