Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

April 20, 2022

# Controlled Access Programs of the Intelligence Community

## Introduction

The Controlled Access Programs (CAPs) that the Intelligence Community (IC) has developed to further limit the sharing of the most sensitive classified information have raised questions for Congress. In response, as part of the Intelligence Authorization Act (IAA) for Fiscal Year 2022, (Division X of P.L. 117-103, the Consolidated Appropriations Act for Fiscal Year 2022) Congress added new oversight requirements with respect to these programs.

CAPs compartmentalize intelligence on the basis of the sensitivity of the activity, sources, or methods involved. Congressional concern has centered on the over-classification of intelligence and potential negative impacts of keeping materials from those who need to know in order to perform their duties. Recent legislation seeks to promote an appropriate balance between protecting the most sensitive sources, methods, and activities, while making sure information is shared with those who have a legitimate need for it. Effective oversight of CAPS may require an understanding of how these programs are authorized and administered, and how they intersect with other classification programs and schema.

## Definitions

Intelligence Community Directive (ICD) 906, *Controlled Access Programs*, provides guidance for management of CAPs and defines a CAP as "a top-level control system and any compartment or sub-compartment under that control system." Within the IC, the topmost level within a CAP structure is called a control system. Common examples of control systems include SI (Special Intelligence), TK (Talent Keyhole), and HCS (Human Intelligence Control System). Control systems can have compartments and sub-compartments.

The names for many CAPs are unclassified, and, in some cases, known to the public (their substance is classified). There are, however, also *unacknowledged* CAPs. These are CAPs whose existence is known only to those who are authorized for access to the information.

Outside of the Intelligence Community the equivalent term for similarly sensitive programs is Special Access Program (SAP). Executive Order (E.O.) 13526, *Classified National Security Information*, defines a SAP as "a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level." Although CAP is the IC term for a SAP, CAPs are managed separately from the SAPs established under the authority of the National Security Council (NSC) or the non-IC components of the Departments of Defense, Justice, Homeland Security, State, and Energy.

## CAPs vs. Classification Levels

A CAP is not a level of classification. A CAP is a compartmentalized control system within a level of classification, involving compartments and sub-compartments. Levels of classification include TOP SECRET, SECRET, and CONFIDENTIAL indicating the relative sensitivity of intelligence activities, sources and methods described within, and the relative damage to United States national security that could result from the document's unauthorized disclosure. Within the IC, CAPs are most commonly compartments or sub-compartments of the TOP SECRET level of classified intelligence.

## CAPs vs. Dissemination Controls

CAPs are not the same as dissemination controls. Dissemination controls are markings appended to the security classification that provide guidance on additional restrictions on access to, or dissemination of, a document. Common dissemination control markings include ORCON (the document's originator controls further dissemination), PROPIN (contractor proprietary information), REL TO (releasable to a particular foreign partner(s)), IMCON (controlled imagery), RELIDO (releasable by a designated Intelligence Disclosure Official), and NOFORN (U.S.-only; no foreign dissemination). Separate dissemination control markings exist for non-intelligence information.

## Authority for Establishing a CAP

ICD 906 specifies that the Director of National Intelligence (DNI) and the Principal Deputy Director of National Intelligence (PDDNI) have the authority to "create, validate, substantially modify, or terminate" a CAP.

ICD 906 also provides that the DNI can delegate to a CAP Program Manager, via the head of any of the 18 statutory IC elements, the authority to "create, substantially modify, or terminate" compartments or sub-compartments of an established control system.

The Intelligence Authorization Act for Fiscal Year 2022 (Division X of P.L. 117-103, the Consolidated Appropriations Act for Fiscal Year 2022) requires that the head of an IC element notify Congress prior to establishing a CAP.

## Standards for Establishing a CAP

Under ICD 906, establishment of a CAP requires (1) a finding that "the vulnerability of, or threat to, specific information is exceptional," such that the normal criteria for determining eligibility for access to information classified at the same level are insufficient to protect the information

from unauthorized disclosure; or (2) Congress to direct the establishment of a CAP through legislation.

## CAP Administration and Oversight

The DNI must validate each CAP at least annually. CAPs not validated within a year are to be terminated.

CAP Program Managers, within an IC element, are responsible for administering CAPs. They also establish the appropriate level of protections for a CAP within the minimum and maximum limits established by the DNI or PPDNI. The CAP Program Manager designates a CAP Control Officer (CAPCO) for routine administration, and the enforcement of policy and procedures related to the execution of the program.

An IC Senior Review Group (SRG) reviews control systems and their compartments and sub-compartments for whether they should be validated, substantially modified, or terminated. On the basis of the findings of the SRG, an IC CAP Oversight Committee (CAPOC), which meets aperiodically, makes recommendations to the DNI on the creation, validation, substantial modification, or termination of control systems.

For the purposes of conducting CAP oversight within the Executive Branch, E.O. 13526, which provides for the administration of classified national security information, allows for the Director of the Information Security Oversight Office (ISOO) of the National Archives and Records Administration (NARA) and no more than one other ISOO employee be given access to a CAP. For CAPs that are "extraordinarily sensitive and vulnerable" access may be limited to the ISOO director alone.

The names of personnel granted access to a CAP are to be kept in the designated IC database that serves as the repository for verifying and validating individual CAP access.

## Congressional Oversight

Congress has acted to supplement IC and NARA oversight measures for CAPs in order to have a better understanding of the purpose and impact of these sensitive programs. The Intelligence Authorization Act (IAA) for Fiscal Year 2022 requires that each IC element provide a baseline report giving information on each CAP, to include for each program the date it commenced, its rationale, annual funding, and current operational use. The report is to go to congressional intelligence and appropriations committees and to Senate and House leadership.

In addition, the IAA for FY2022 requires the head of each IC element to submit an annual report to the congressional intelligence and appropriations committees of the Senate and House of Representatives on CAPs the element administers. The reports are to include (1) a list of the compartments and sub-compartments for each CAP that is either active or was terminated during the previous year; and (2) (for the annual report submitted by the DNI), a *certification* of whether the creation, validation, substantial modification, or termination of each CAP is "substantiated and justified."

The IAA also requires that the DNI provide briefings on each CAP at least semiannually or as requested by the congressional intelligence and appropriations committees or House and Senate leadership. The briefings are to include a description of the activity during the reporting period and the extent to which it has satisfied the requirements that initially justified establishing the program.

### Statutory IC Elements with Authority for the Administration and Oversight of CAPs

**DOD Elements:**

- Defense Intelligence Agency (DIA)
- National Geospatial-Intelligence Agency (NGA)
- National Reconnaissance Office (NRO)
- National Security Agency (NSA)
- U.S. Air Force Intelligence, Surveillance and Reconnaissance (AF/A2)
- U.S. Space Force Intelligence (S-2)
- U.S. Army Intelligence (G2)
- U.S. Marine Corps Intelligence, Surveillance and Reconnaissance Enterprise (MCISR-E)
- U.S. Naval Intelligence (N2)

**Non-DOD Elements:**

- Office of the Director of National Intelligence (ODNI)
- Central Intelligence Agency (CIA)
- Department of Energy (DOE) intelligence component: Office of Intelligence and Counter-Intelligence (I&CI)
- Department of Homeland Security (DHS) intelligence components: Office of Intelligence and Analysis (I&A) and U.S. Coast Guard Intelligence (CG-2)
- Department of Justice (DOJ) intelligence components: the Drug Enforcement Agency's Office of National Security Intelligence (DEA/ONSI) and the Federal Bureau of Investigation's Intelligence Branch (FBI/IB)
- Department of State (DOS) intelligence component: Bureau of Intelligence and Research (INR)
- Department of the Treasury intelligence component: Office of Intelligence and Analysis (OIA)

### Related CRS Products

CRS Report R45421, *Congressional Oversight of Intelligence: Background and Selected Options for Further Reform*, by Michael E. DeVine

CRS In Focus IF10525, *Defense Primer: National and Defense Intelligence*, by Michael E. DeVine

### Relevant Legislation

Intelligence Authorization Act for Fiscal Year 2022 (Division X of the Consolidated Appropriations Act for Fiscal Year 2022, P.L. 117-103)

### Other Resources

ICD 906, Controlled Access Programs

E.O. 13526, Classified National Security Information

E.O. 12333, United States Intelligence Activities

Controlled Access Program Coordination Office (CAPCO) Register and Manual

**Michael E. DeVine**, Analyst in Intelligence and National Security

**IF12080**

## Disclaimer