Department of Homeland Security
DHS Directives System
Directive Number: 140-04
Revision Number: 00
Issue Date: 08/12/2009

SPECIAL ACCESS PROGRAM MANAGEMENT

I. Purpose

This Directive establishes the Department of Homeland Security (DHS) policy for the management and administration of DHS Special Access Programs (SAPs). It establishes the DHS Special Access Program Oversight Committee (SAPOC), and the Special Access Program Control Office (SAPCO) in order to accomplish planning, organizing, directing and overseeing both DHS originated SAPs and the Department's participation in non-DHS SAPS. It also outlines the specific responsibilities which DHS must accomplish to comply with Executive Order (E.O.) 12958, as amended.

II. Scope

A. This Directive applies throughout DHS to DHS personnel who require access to DHS SAPs, or who participate in non-DHS SAPs.

B. DHS Management Directive 10150, "Research, Development, Testing and Evaluation Special Access Programs," is hereby canceled.

III. Authorities

A. Executive Order 12958, as amended, "Classified National Security Information," April 17, 1995

B. Executive Order 13292, "Further Amendment to Executive Order 12958, as amended, Classified National Security Information," March 25, 2003

C. Executive Order 12968, as amended, "Access to Classified Information," August 2, 1995

D. Executive Order 12829, as amended, "National Industrial Security Program," January 6, 1993

E. . Title 6, Code of Federal Regulations, § 7.10, "Authority of the Chief Security Officer, Office of Security"

F. Memorandum from the Assistant to the President for National Security

Affairs to The Secretary of Homeland Security, "Special Access Programs," January 17, 2005

G. Information Security Oversight Office (ISOO), "Classified National Security Information Directive No. 1," September 22, 2003.

IV. Definitions

A. ***Non-DHS SAPs***: Are those SAPs either established by, under the cognizance of, or administered by other federal agencies or departments. This definition includes foreign government Special Access Programs.

B. ***Participation or Significant Activity***: An activity beyond a simple awareness of the existence of a SAP (e.g., committing DHS resources in either personnel or funds).

C. ***Senior Agency Official (SAO)***: The official designated by the agency head under section 5.4(d) of E.O. 12958, to direct and administer the agency's program under which information is classified, safeguarded, and declassified. The Senior Agency Official is specifically responsible for the oversight of DHS participation in special access programs authorized under E.O. 12958. The Senior Agency Official for DHS is the Chief Security Officer (CSO).

D. ***Special Access Program (SAP)***: Is a program established for a specific class of classified information that imposes safeguarding, need-to-know, and access requirements in excess of those normally required for information at the same classification level.

V. Responsibilities

A. The ***Deputy Secretary***:

1. Serves as the Chairman of the Special Access Program Oversight Committee (SAPOC) and renders all final decisions for the establishment or disposition of all SAPs within the Department.

2. Approves the release of SAP information outside the Department, after coordination with the SAPOC and the SAPCO.

3. Approves a Component head, when properly cleared and briefed, to serve as an ad hoc member of the SAPOC. Substitutions are not below the Component head's principal deputy, and are approved in advance by the Deputy Secretary.

B. The ***Chief Security Officer***, in the designated role as the SAO for DHS, oversees DHS SAPs and DHS participation in non-DHS SAPs.

C. The ***Special Access Program Oversight Committee (SAPOC)***:

1. Makes recommendations as to the approval, conduct, and disposition of all SAPs within the Department.

2. Consists of the Deputy Secretary (Chair), the General Counsel, the Under Secretary for Management, the Under Secretary for Intelligence and Analysis, the CSO, the Chief of the SAPCO (Executive Secretary) and the Under Secretary or equivalent official from the Component proposing the SAP (ad hoc member).

3. Reviews all DHS SAP activities annually, via the annual report, and validates the continuing need or discontinuation for each SAP and the Department's involvement with and commitment to non-DHS SAPs.

D. ***Component heads:*** designate a single point of contact within the Component for all matters relating to SAPs, and work with procurement officials to ensure all contracts contain appropriate language to require compliance with the applicable provisions of this Directive when the contractor needs access to SAPs.

E. The ***DHS Inspector General (or other DHS officers with specific statutory oversight responsibilities)*** may conduct, in coordination with the SAPCO, investigations, audits or inspections of DHS Special Access Programs. Such investigations, audits or inspections are conducted using cadres of appropriately vetted DHS personnel who have proper security clearances and have been approved for SAP access.

VI. Policy & Requirements

A. The Secretary and the Deputy Secretary are responsible for all SAP activities within the Department and are the only officials within the Department authorized to approve the establishment or termination of DHS Special Access Programs, or the commitment of DHS resources to participate in a non-DHS SAP.

B. ***General***:

1. DHS establishes and maintains SAPs on a case-by-case basis and in cooperation with the Director of ISOO, only when the program does not involve intelligence sources and methods (as such programs fall under the cognizance of the Director of National Intelligence), and only when the SAP meets and is executed consistent with the requirements of Section 4.3. of E.O. 12958, as amended.

2. Minimum personnel security requirements for access to DHS SAPs are a final Top Secret clearance based on a personnel security investigation that is current within five years (in scope) and has been adjudicated to ICD-704 standards. Exceptions, waivers, deviations or the use of an interim security clearance for granting access to DHS SAPs is not authorized unless specifically approved by the Chief of the SAPCO. On a case-by-case basis, the SAPOC may approve additional personnel security requirements upon establishing a SAP.

3. The number of persons granted access to a SAP is strictly limited to the minimum necessary for the execution of the program. Granting access to a DHS SAP is based solely upon a determination that the individual has a valid need-to-know, has the requisite security clearance, meets approved personnel security requirements for access, and clearly and materially contributes to the execution or oversight of the program. Individuals are not granted SAP access based solely upon rank, position or title.

4. An individual with an existing DHS SAP access, granted without exception, condition or waiver, is considered eligible for access to another DHS SAP, of the same sensitivity level, as long as the individual has a validated need for access to the information involved.

5. All personnel having access to DHS SAPs are subject to a random Counterintelligence (CI)-scope polygraph examination. However, using a polygraph examination as a determinant for access is a condition specifically approved by the Secretary or the Deputy Secretary in conjunction with the establishment of the SAP. In such cases, the polygraph examination is consistently applied to all candidates. CI-scope polygraph examinations are not used as the only basis for granting access to DHS SAPs. The polygraph may be used to obtain exculpatory information in those instances when a personnel security investigation can not be completed in a timely manner.

6. DHS personnel with legal, fiscal, investigative, operational or statutory oversight responsibilities for SAPs are deemed to have a need-to-know for access. Following a favorable personnel security

determination, those personnel are granted effective and sufficient access to meet their functional responsibilities. This support is provided by cadres of specifically-dedicated and vetted DHS government personnel.

C. ***Security Violations and Infractions***:

1. Incidents involving the security, mishandling, compromise, or suspected compromise of SAP information are promptly reported to the SAPCO and thoroughly investigated within SAP security channels to determine the cause, assess and mitigate potential damage, and implement measures to prevent recurrence.

2. Actions, to include suspending or revoking an individual's access, may be imposed when an individual is found to be culpable for the commission of a security infraction or violation.

D. ***Fraud, Waste, Abuse or Mismanagement (FWA)***: DHS employees, contractors, sub-contractors or consultants who suspect or have knowledge of fraud, waste, abuse or mismanagement involving DHS SAPs may report such to the DHS OIG Hotline at 1-800-323-8603. DHS OIG personnel are not routinely briefed into SAPs unless or until there is a functional reason to do so; therefore, special care must be exercised when making reports not to compromise SAP information (i.e., the inadvertent disclosure of SAP information).

VII. Questions

Address any questions or concerns regarding this Directive to the Office of the Chief Security Officer, attention: Chief, Special Access Programs Control Office (SAPCO).

Janet Napolitano
Secretary of Homeland Security

8-12-05
Date