

INSTRUCTION FOR THE OFFICE OF THE CHIEF SECURITY OFFICER

I. Purpose

This Instruction establishes procedures, program responsibilities and reporting protocols to implement the Department of Homeland Security (DHS) Directive 121-01, Chief Security Officer.

II. Scope

This Instruction applies throughout DHS, except where exempted by statute. However, as part of the larger DHS team, even exempted DHS Components will collaborate and participate in the efforts described herein to further both operational and organizational effectiveness and efficiency, and to ensure their security policies and procedures are in concert with the Chief Security Officer (CSO) security objectives.

III. Background

The CSO develops, implements, and oversees the Department's security policies, programs, and standards; delivers security training and education to DHS personnel; and provides security support to Components. The CSO generally accomplishes these tasks through the Office of the Chief Security Officer (OCSO). Working with the Chief Security Officer (CSO) Council, the OCSO integrates all security programs for DHS in a cohesive manner that increases efficiency and enhances the overall security of DHS.

IV. Definitions

- A. **Classified National Security Information ("classified information")**: Information that has been determined, pursuant to Executive Order 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

B. **Component Chief Security Officers**: The senior-most federal security official designated by the Component head in the following Components:

1. U.S. Citizenship and Immigration Services (USCIS)
2. U.S. Coast Guard (USCG)
3. U.S. Customs and Border Protection (CBP)
4. Federal Emergency Management Agency (FEMA)
5. Federal Law Enforcement Training Center (FLETC)
6. U.S. Immigration and Customs Enforcement (ICE)
7. U.S. Secret Service (USSS)
8. Transportation Security Administration (TSA)

C. **CSO Council**: The DHS functional advisory body that assists the DHS CSO in evaluating and determining the best course of action for the security program. The CSO Council is chaired by the DHS CSO and includes the CSOs of each Component.

D. **CSO-Serviced Facility**: DHS facilities which are occupied by the Office of the Secretary and Components, and are provided security-related services by the OCSO, to include space provided by the General Services Administration, space owned or leased directly by a Component, or space provided by any other entity.

E. **Counterintelligence**: As defined in Title 50, Chapter 15, § 401a means information gathered and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or persons, or international terrorist activities.

F. **DHS Chief Security Officer**: The DHS official in charge of the OCSO and who exercises leadership and authority over security policy and programs DHS-wide in partnership with Component heads.

G. **Intelligence Community**: As defined in the National Security Act of 1947, as amended, the Intelligence Community is a federation of executive branch agencies and organizations that conduct intelligence activities necessary to carry out foreign relations and the protection of the national security of the United States.

H. **Key Security Officials (KSOs)**: The senior-most federal security official designated by the Component head in, accordance with DHS Management Directive 11080, in each of the following Components

1. Domestic Nuclear Detection Office (DNDO)
2. Intelligence and Analysis, Office of (I&A)
3. Science and Technology (S&T)

I. **Security Program**: The personnel resources, assets, budgets, and processes used to deliver mission and services to protect and safeguard DHS's personnel, property, facilities, and information. The security program includes the areas of personnel security, physical security, administrative security, special security programs, counterintelligence and investigations, security training and awareness and operations security.

J. **Sensitive Compartmented Information (SCI)**: As defined in Director of Central Intelligence Directives (DCID) 6/3, 6/4, and 6/9, SCI is classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled exclusively within formal control systems established by the Director of National Intelligence.

K. **Sensitive Compartmented Information Facility (SCIF)**: As defined in DCID 6/9, a SCIF is an accredited area, room, group of rooms, building(s), or installation where SCI may be stored, used, discussed, and/or electronically processed.

L. **Special Access Programs**: Special Access Programs (SAPs) are individual and independent programs established for a specific class of classified information that impose safeguards, need-to-know and access requirements in excess of those normally required for information at the same classification level.

V. Responsibilities

A. The **Chief Security Officer** is responsible for:

1. Developing and implementing security policies, programs, and standards to protect and safeguard the Department's personnel, property, facilities, and information.
2. Publication of DHS instructions in the areas of personnel security, physical security, administrative security, special security programs, counterintelligence operations, security-related investigations, and security training and awareness.

3. Integrating, coordinating and providing oversight of Component security policies, programs, and standards to protect and safeguard DHS Component personnel, property, facilities, and information.
4. Providing direct security support and services to all Components not serviced by, or under the jurisdiction of, a Component CSO.
5. Representing DHS on security-related interagency committees and working groups.
6. Exercising policy oversight of Component programs related to the protection of property owned or occupied by the Federal Government and persons on the property.
7. Exercising policy oversight of Component programs related to credentials, badges, emergency signaling devices, and other law enforcement-related signifiers.
8. Coordinating with the Office of Inspector General (OIG) on OIG investigations relating to matters impacting the ability of a DHS employee or contractor to maintain a security clearance, and receiving the final Report of Investigation (ROI) and all related exhibits upon issuance to the affected Component. Likewise, when the OCSO is responsible for conducting investigations of allegations against employees, as detailed in MD 0810.1, Office of Inspector General, OCSO will coordinate open investigations, and, upon request, provide OIG with completed Reports of Investigations, including all exhibits.
9. Ensuring that a Security Appeals Board is convened to address appeals made by a DHS applicant or employee after a decision to deny or revoke a security clearance has been affirmed.

B. The **Chief of the Personnel Security Division within the OCSO** is responsible for:

1. Personnel security and suitability policies, programs, and standards, including procedures for granting, denying and revoking access to classified information.
2. Initiating and adjudicating personnel security and suitability background investigations and periodic reinvestigations of applicants and appointees.
3. The Contractor Suitability Program, which ensures suitability screening standards for U.S. industry partners performing work for DHS.

4. The process for issuing access eligibility to classified information to state, local and tribal government officials and private-sector individuals.
5. Adjudication of employee and contractor eligibility for access to SCI.
6. Serving as the first-level deciding authority for the Office of the Secretary and those Components without a personnel security office for making initial eligibility or suspension determinations of access to classified information and notifying the applicant or employee of the determination.

C. The **Chief of the Administrative Security Division within OCSO** is responsible for:

1. Policies, programs, and standards necessary to ensure the protection of collateral classified and sensitive but unclassified information.
2. Self-inspection programs that ensure classified and sensitive information is protected.
3. A comprehensive, multi-disciplined program to ensure that employees are educated on the responsibilities and restrictions associated with the classification, safeguarding, and declassification of information.
4. Publication of security classification guides.
5. A program that ensures the protection of classified information provided to state, local and tribal government officials and private-sector individuals.
6. The DHS Industrial Security Program, which ensures that industry partners with access to classified information comply with the standards for safeguarding such information.
7. Support for the Office of the Chief Information Officer (OCIO) on the development and deployment of classified information technology systems.

D. The **Chief of the Physical Security Division within OCSO** is responsible for:

1. Physical security policies, programs, and standards for DHS facilities, to include access control card programs and security guard forces.

2. The Technical Security Countermeasure (TSCM) Program for DHS facilities, which includes techniques used to detect and nullify unauthorized access to classified national security information, restricted data, or sensitive information.
3. Support for the accreditation of SCIFs.
4. Installation and operation of surveillance equipment for CSO-serviced facilities.
5. Homeland Security Presidential Directive 12 (HSPD-12) requirement to implement common identification standards for federal employees and contractors – (Smart Cards).

E. The ***Chief of the Special Security Programs Division (SSPD) within OCSO*** is responsible for:

1. Security policy oversight and programs for protecting information received from the Intelligence and Special Access Communities.
2. The SCI program within DHS.
3. DHS participation in, and support of, SAP facilities and information systems.
4. The Special Security Officer (SSO) Program which provides direct, on-site support to DHS Components' SCI programs.
5. Support to the DHS Designated Accreditation Authority (DAA) for the certification and accreditation of intelligence information systems and DCID 6/3 compliance.
6. Support to DHS Components to ensure compliance with, and standardization of, DHS special security programs.
7. Concept approval, requirements analysis, and certification and accreditation of DHS SCIFs.
8. Liaison with the Intelligence Community and organizations with SAPs on security-related activities and issues.

F. The Chief of the **Counterintelligence and Investigations Division (CIID) within OCSO** is responsible for:

1. Security audits, inspections, and investigations involving alleged crimes against DHS or its employees, and allegations of illegal activities by DHS personnel. These activities relating to the security program will be closely coordinated with the investigations of fraud, waste, and abuse conducted by the Office of Inspector General (OIG) in accordance with DHS Management Directive (MD) 0810.1, Appendix A. If OIG declines to investigate criminal allegations involving Components that do not have investigative authorities or capabilities, it refers those allegations to the OCSO.
2. Security policies, program, and standards as outlined in DHS MD 11052.
3. Programs to address security requirements for foreign travel by DHS personnel, contacts with foreign nationals by DHS personnel, and visits to DHS facilities by foreign nationals.
4. Providing investigative and liaison support to the Intelligence Community on security matters affecting DHS. Conducting inquiries of counterintelligence incidents and anomalies, in coordination with component intelligence/security organizations as appropriate. Determining if an incident should result in a referral to the Federal Bureau of Investigation (FBI) pursuant to Section 811 (c) of the Intelligence Authorization Act of 1995.
5. Operational control and day-to-day execution of the Counterintelligence activities of the OSCO.
6. Working with the Office of Intelligence & Analysis to develop Counterintelligence policies, plans, and strategies.
7. Maintaining operational liaison with other intelligence agencies, counterintelligence agencies, and law enforcement organizations for counterintelligence and law enforcement matters.

G. The **Chief, Training and Operations Security Division within OCSO** is responsible for:

1. Integrating Departmental security training policy and programs across all security disciplines.
2. Providing publications of security training, education and awareness products.

3. Integrating Departmental applied operations security (OPSEC) policy and programs across all DHS Components and affiliates (i.e. state and local, First Responders, private sector).
4. Managing, supporting and coordinating the Office of Security technology systems and related processes.

H. **Component heads** are responsible for:

1. Ensuring that security management duties are carried out effectively and efficiently in support of mission accomplishment and functional integration goals.
2. Supporting and implementing the annual security program goals established in collaboration with the DHS CSO.
3. Ensuring that the structure and organization of the security program is aligned with security best practices, as determined by the CSO Council.
4. Advising and collaborating with the DHS CSO on any Component reorganization or restructuring plans that will result in security program realignments.
5. With the DHS CSO, and through their Component CSO, collaborating to ensure that the appropriate security resources are made available for Department-wide security programs and providing the direction required to achieve security program excellence.

I. **Component Chief Security Officers and Key Security Officials** are responsible for:

1. Serving as the principal advisor to their Component head on security issues.
2. Ensuring that security programs meet the mission needs of DHS and the Component.
3. Advising (e.g., in writing or orally) the DHS CSO concerning the security requirements of their Component.
4. Advising and partnering within their respective Component to ensure that security staffs provide quality and timely support to mission requirements.

5. Participating in the development of DHS-wide security directives and policies as members of the CSO Council, and implementing DHS-wide security directives and policies within their respective Component.
6. Coordinating with their respective intelligence chiefs, special security officer, and the SSPD in the development of security policies to ensure appropriate consideration of protection requirements for SCI.
9. Developing and reviewing the Component security budget formulation and execution to include preparing a separate security budget, starting with Fiscal Year 2011, using the Resources Allocation Plan (RAP) Over-Guidance Submission instruction provided by the DHS CFO. This will include the security budget across all programs and activities within the Component.

J. The **CSO Council** is responsible for:

1. Development of a Departmental security strategic plan and establishment of priorities for the security program.
2. Security assessment and accountability, which includes coordination and consolidation of Component security projects/activities and implementation of shared services as appropriate.
3. Security management policies, processes, best practices, performance measures, and decision criteria for managing the delivery of security programs to enhance efficient and effective security management.
4. Implementing Security Centers of Excellence, boards, working groups and resource sharing tied to DHS CSO Council priorities and to continuously improve DHS security processes and performance.

VI. Guiding Principles and Procedures

The CSO will:

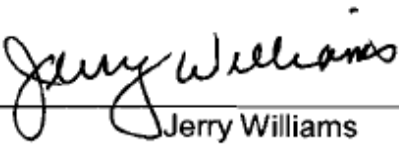
- A. Standardize security policies and appropriate procedures across DHS to ensure functional excellence;
- B. Consolidate and integrate systems supporting DHS's security programs, ensuring such action results in efficiencies and does not compromise mission effectiveness;
- C. Consolidate organizations that perform the same function and create centers of excellence, ensuring such action results in efficiencies and does not compromise mission effectiveness;

D. In collaboration with the Component heads and CSO Council, establish annual milestones for the functional integration of security programs; and

E. Ensure the use of Department-wide performance standards and metrics to track security program effectiveness across the Department.

VII. Questions

Address all questions or concerns regarding this Instruction to the Office of the Chief Security Officer.



Jerry Williams
Chief Security Officer

9-3-08

Date