Department of Homeland Security
Management Directives System
MD Number: 11005
Issue Date: 3/23/2006

SUSPENDING ACCESS TO DHS FACILITIES, SENSITIVE INFORMATION, AND IT SYSTEMS

I. Purpose

This Management Directive (MD) establishes the policy, procedures, standards, and requirements for suspending access to Department of Homeland Security (DHS) facilities, sensitive information, and information technology (IT) systems.

II. Scope

This MD applies to all DHS Components and the immediate Office of the Secretary. Any DHS Component that has existing procedures, standards, and requirements regarding the suspension of physical and systems access may continue them in force.

III. Authority

A. Homeland Security Act of 2002, as amended.

B. DHS Management Directive 11042.1, "Safeguarding Sensitive But Unclassified (For Official Use Only) Information."

C. DHS Management Directive 4300.1, "Information Technology Systems Security."

D. DHS Sensitive Systems Policy Directive 4300A

IV. Definitions

A. ***Access***: The ability, means, or opportunity to gain knowledge of information; the ability to enter DHS facilities.

B. ***Components***: All the entities that directly report to the Office of the Secretary, which includes the Secretary, Deputy Secretary and Chief of Staff.

C. ***DHS Facility***: A DHS-owned buildings or leased space, whether for single or multi-tenant occupancy, and its grounds and approaches, all or any portion of which is under the jurisdiction, custody, or control of the Department; DHS-controlled commercial space shared with non-government tenants; DHS-owned contractor-operated facilities; and facilities under a management and operating contract such as for the operation, maintenance, or support of a Government-owned or controlled research, development, special production, or testing establishment.

D. ***DHS Sensitive Systems***: Any information technology system that stores, processes, or manipulates DHS sensitive information.

E. ***Immediate Office of the Secretary***: the Secretary and his or her staff, the Deputy Secretary and his or her staff, the Chief of Staff and his or her staff, and the Counselors.

F. ***Information Technology (IT)***: As defined by 40 U.S.C. § 11101(6) ("Clinger-Cohen Act"), any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by DHS. This definition applies if the equipment is used by DHS directly or is used by a contractor under a contract with DHS that requires the use of that equipment; or of that equipment to a significant extent in the performance of a service or the furnishing of a product. The definition includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

G. ***IT Systems***: Information technology systems that are (1) owned, leased, or operated by a Component; (2) operated by a contractor on behalf of DHS; or (3) operated by another Federal, state, or local government agency on behalf of DHS.

H. ***Sensitive Information***: This definition includes the following categories of information:

1. For Official Use Only (FOUO): information not otherwise categorized by statute or regulation, the loss, misuse, disclosure, unauthorized access to, or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria by an Executive Order or an Act of Congress to be kept secret in the interests of national defense, homeland security, or foreign policy.

2. Protected Critical Infrastructure Information (PCII) as described in the Critical Infrastructure Information Act of 2002, 6 U.S.C. section 211-224; its implementing regulations, 6 C.F.R. Part 29; or the applicable PCII Procedures Manual;

3. Sensitive Security Information (SSI), as described in 49 C.F.R. Part 1520;

4. Information that is designated "sensitive" in accordance with subsequently adopted homeland security information handling requirements.

V. Responsibilities

A. ***The Chief Security Officer (CSO)*** is responsible for:

1. Suspending an individual's access to DHS facilities, and to sensitive information, including that which resides on DHS information technology systems, when conditions exist that raise a security concern;

2. Ensuring that the Office of Inspector General (OIG) is notified of all alleged or suspected security incidents, in accordance with MD 0810.1.

3. Ensuring that all actions are coordinated with the Office of General Counsel as appropriate.

B. ***The Chief Information Officer (CIO)*** is responsible for:

1. Suspending an individual's access to DHS sensitive systems when conditions exist that raise a security concern;

2. Ensuring the OIG is immediately notified of all alleged or suspected security incidents, in accordance with MD 0810.1;

3. Ensuring that all actions are coordinated with the Office of General Counsel as appropriate.

C. ***The Chief Human Capital Officer (CHCO)*** is responsible for:

1. Providing technical expertise and counsel regarding personnel rules, regulations, and procedures to help the Chief Security Officer and the Chief Information Officer choose a course of administrative action that is most appropriate in specific situations;

2. Assisting in implementing appropriate administrative or corrective action as a result of a determination to suspend access.

D. ***The Chief Procurement Officer (CPO)*** is responsible for:

1. Ensuring that contracts and grants involving access to facilities, information and systems comply with the appropriate security policies, procedures, and guidelines;

2. Providing expertise regarding contracts and grants to assist the Chief Security Officer and Chief Information Officer determine a course of action that is appropriate in specific situations.

E. ***Supervisors and Managers*** are responsible for identifying and immediately reporting to security personnel situations or risk factors that may give rise to security concerns.

F. ***All DHS personnel*** are responsible for complying with this MD and reporting to appropriate officials any situations that may give rise to security concerns.

VI. Policy & Procedures

A. ***Policy***.

1. The CSO is authorized to suspend access to DHS facilities, and to sensitive information, including that which resides on information technology systems.

2. The CIO is authorized to suspend access to DHS sensitive systems. The CIO is required to suspend access to sensitive systems when the CSO suspends access to DHS facilities, or sensitive information, or both.

3. A suspension is an administrative procedure. Access to DHS facilities and sensitive systems may be suspended based on conditions that raise a security concern. Suspension of access also may be appropriate when there is a reasonable belief that the individual's continued access to DHS's facilities and its sensitive information and systems is not in the interest of the Department. The CSO and/or CIO will take into consideration any identified mitigating factors when making this decision.

4. Conditions that raise a security concern include, but are not limited to the following:

a. Revocation of security clearance;

b. Questionable allegiance to the United States;

c. Susceptibility to foreign influence or preference;

d. Personal conduct indicating questionable judgment, untrustworthiness, unreliability, lack of candor, and unwillingness to comply with rules and regulations. This includes:

(1) Unauthorized release of proprietary , sensitive, or other government-protected information;

(2) Disruptive, violent, or other inappropriate behavior in the workplace;

(3) A pattern of dishonesty or rule violations;

(4) Evidence of significant misuse of Government time or resources;

(5) Association with persons involved in a criminal activity.

e. Financial instability;

f. Excessive alcohol consumption;

g. Improper or illegal involvement with drugs;

h. Certain emotional, mental, and personality conditions. (A duly qualified mental health professional employed by, or acceptable to and approved by the U.S. Government should be consulted when evaluating these conditions. No negative inference may be raised solely on the basis of seeking mental health counseling);

i. Criminal conduct;

j. Noncompliance with security regulations;

k. Certain types of outside employment or activities, including but not limited to any employment or service, whether compensated or volunteer with:

(1) The government of a foreign country;

(2) Any foreign national, organization, or entity;

(3) A representative of any foreign interest;

(4) Any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology;

l. Misuse of information technology systems.

5. All actions to suspend access to DHS facilities or sensitive systems, or both, will be coordinated among the Office of Security, the Office of the Chief Information Officer, the Office of the Chief Human Capital Officer, the Office of the Chief Procurement Officer, and the Office of General Counsel, as appropriate.

6. The CSO or CIO, or both, will report suspension of access to the individual's immediate supervisor and make other notifications as may be warranted.

7. The immediate supervisor will notify the individual.

8. If the individual is a contractor employee, the CSO or CIO will report the suspension of access to the Contracting Officer and Contracting Officer's Technical Representative (COTR). The Contracting Officer and COTR will administer the suspension, including, but not limited to, coordinating with the Project Manager or company representatives, or both.

9. When access to DHS facilities, sensitive information, or sensitive systems has been suspended, the CSO or CIO shall attempt to resolve the case as expeditiously as circumstances permit, aiming to do so within 90 days from the date of suspension, or within 60 days from the conclusion of an investigation. All actions taken during this process will be documented.

10. Final disposition issues will be handled on a case-by-case basis in coordination with CHCO, OGC, and CPO as appropriate.

11. Nothing in this directive shall limit the authority of the Office of Inspector General as prescribed under DHS MD 0810.1 and the Inspector General Act of 1978, as amended.

B. ***Procedures***.

1. Physical Access

a. When access to a DHS facility is suspended, authorized Office of Security personnel or their designees will complete the following actions as soon as possible, but no later than the next business day from the time of suspension:

(1) Retrieve all keys, access control cards/badges, and other access devices that afford the individual access to DHS facilities.

(2) Suspend access through all electronic access control devices and access control lists.

(3) Change combinations to all locks to which the individual has access, as soon as possible, but no later than two business days from the time of suspension.

b. All retrieved items will be held in a secure location until a final resolution is reached.

2. Sensitive Systems Access

a. When access to DHS sensitive systems is suspended, authorized systems security personnel or designated system administrator will complete the following actions as soon as possible, but no later than the next business day from the time of suspension:

(1) Suspend all access authorizations.

(2) Retrieve all devices that afford access to DHS sensitive systems.

(3) Retrieve all government-owned, leased, or sponsored equipment that affords access to DHS sensitive systems.

b. All accesses will be disabled and equipment held in a secure location until a final resolution is reached.

3. Supervisors will retrieve all other sensitive government property and information. This property will be held in a secure location until a final resolution is reached.

VII. QUESTIONS

Questions regarding this MD should be addressed to the DHS Office of Security.