Department of Homeland Security
DHS Directives System
MD Number: 140-01
Revision Number: 00
Issue Date: 07/31/2007

INFORMATION TECHNOLOGY SYSTEMS SECURITY

I. Purpose

This directive establishes Department of Homeland Security (DHS) policy regarding Information Technology (IT) Systems Security.

II. Scope

A. This directive applies to all DHS organizational elements.

B. The DHS IT Security Program does not apply to any IT system that processes, stores, or transmits foreign intelligence information pursuant to Executive Order (E.O.) 12333 or subsequent orders.

C. This directive addresses IT Systems Security only; management directives on personnel, physical, information, and industrial security; emergency preparedness; and domestic counter terrorism will be issued separately.

III. Authorities

This directive is governed by numerous Public Laws, Executive Orders (E.O.), regulations, Presidential Decision Directives (PDD), agency manuals, and Office of Management and Budget (OMB) circulars, such as:

A. P.L. 100-235.

B. P.L. 107-296, Homeland Security Act of 2002, Title X, Federal Information Security Management Act (FISMA) of 2002.

C. P.L. 107-347, E-Government Act of 2002, Title III, Federal Information Security Management Act (FISMA) of 2002.

D. OMB Circular A-130, Management of Federal Information Resources.

E. P.L. 104-106, Clinger-Cohen Act of 1996, as amended [formerly, Information Technology Management Reform Act (ITMRA).

F. Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a.

G. E.O. 13231, Critical Infrastructure Protection in the Information Age.

H. PDD 63, Critical Infrastructure Protection.

I. 5 CFR § 2635, Office of Government Ethics, Standards of Ethical Conduct for Employees of the Executive Branch.

J. Department of State 12 Foreign Affairs Manual (FAM) 600, Information Security Technology, June 22, 2000.

IV. Definitions

Definitions of Information Systems Security specific terms are provided in the IT Security Program Publications (attached to this directive).

V. Responsibilities

A. Public Law and Executive Orders place the responsibility for Information Systems Security on ***the Secretary of the DHS and the Chief Information Officer (CIO)***. Additional Public Law requires a ***DHS Chief Information Systems Security Officer (CISSO)***. The IT Security Program Publications (attached to this directive) detail the individual roles and responsibilities as well as subordinate and collateral positions.

B. ***The Under Secretary for Management, through the DHS Chief Information Officer***, shall be responsible for all aspects of this directive.

VI. Policy & Procedures

A. The Department of Homeland Security IT Security Program will serve as a foundation for DHS organizational elements to use in establishing IT security programs within their organizations. The IT Systems Security Program ensures comprehensive, uniform IT security policies are followed by each DHS organizational element. The DHS IT Security Program clarifies national policies, adapts them to specific circumstances, and imposes additional requirements when necessary.

B. All DHS organizational elements are hereby directed to follow guidelines and policies as outlined herein and in the IT Security Program Publications.

C. The IT Security Program Publications attached to this directive:

1. Provide detailed policy and implementation guidance.

2. Identify specific policy and procedures for Sensitive and National Security Systems.

3. Provide policies that relate to management, operational, industrial, and technical controls that provide the foundation to ensure confidentiality, integrity, availability, reliability, and non-repudiation within the DHS IT infrastructure and operations.

D. All documents related to the DHS IT Systems Security Program are living documents. New sections will be developed in the publications to keep pace with advances in technology and policy evolution.

E. Any questions or concerns regarding this directive should be addressed to the Office of the DHS Chief Information Officer.