Department of Homeland Security
DHS Directives System
Directive Number: 140-01
Revision Number: 02
Issue Date: MAY 0 5 2017

INFORMATION TECHNOLOGY SECURITY PROGRAM

I. Purpose

This Directive establishes Department of Homeland Security (DHS) policy regarding the Information Technology (IT) Security Program. Additional DHS policies specific to management, operational, and technical security controls are contained in "DHS Sensitive Systems Policy 4300A" and "DHS National Security Systems Policy 4300B," which are issued by the Under Secretary for Management. Components develop and implement their IT Security Programs pursuant to this Directive and DHS additional IT Security Program policies.

II. Scope

This Directive applies throughout DHS, to all IT systems, including National Security systems.

A. Nothing in this Directive impedes the statutory authority of the Inspector General as set forth in the Inspector General Act.

B. This Directive does not apply to the Office of Intelligence and Analysis intelligence activities.

C. 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.

III. Authorities

A. Public Law 104-106, "Clinger-Cohen Act of 1996"

B. Public Law 107-347, "The E-Government Act of 2002"

C. Public Law 113-283, " Federal Information Security Modernization Act of 2014 (FISMA)"

D. Public Law 113-291, "Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015," Title VIII, "Acquisition Policy, Acquisition Management, and Related Matters," Subtitle D, "Federal Information Technology Acquisition Reform"

E. Title 5, United States Code (U.S.C.), Section 552a, "Records Maintained On Individuals"

F. Title 44, U.S.C., Chapter 35, "Coordination of Federal Information Policy"

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

H. Presidential Decision Directive 63, "Critical Infrastructure Protection"

I. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources"

J. DHS Delegation 00002, "Delegation to the Under Secretary for Management"

K. DHS Delegation 04000, "Delegation for Information Technology"

L. National Institute of Standards and Technology (NIST) Federal Information Processing Standard FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems"

M. NIST Special Publication (SP) 800-53, Rev 4, "Security and Privacy Controls for Federal Information Systems and Organizations"

N. NIST SP 800-37, Rev 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"

IV. Responsibilities

A. The ***Under Secretary for Management***

1. Provides security for information technology and communication systems and a Department-wide IT Security Program;

2. Selects and oversees a multi-component information technology security subject matter expert panel that reviews annually (or as needed) "DHS Sensitive Systems Policy 4300A" and "DHS National Security Systems Policy 4300B" for updates, additions, or changes; and

3. Issues updated "DHS Sensitive Systems Policy 4300A" and "DHS National Security Systems Policy 4300B", after input from the subject matter expert review.

B. The ***DHS Chief Information Officer (CIO)***:

1. Oversees the Department-wide IT Security Program, administered by the Office of the Chief Information Security Officer (OCISO);

2. Appoints the DHS Chief Information Security Officer;

3. Reviews and evaluates the DHS IT Security Program annually;

4. Ensures the DHS network security infrastructure and operations are developed and maintained in accordance with all applicable Federal laws, regulations, Executive Orders, and DHS Directives and policies;

5. Provides feedback to the Component Chief Information Officers on the evaluation of the DHS IT Security Program;

6. Establishes IT Security procedures, including supporting governance structures, consistent with the policies contained within this Directive; and

7. Ensures continuity of operations for information systems that support the operations and assets of the Department.

C. The ***Component Heads*** ensure that an IT Security Program is established and managed in accordance with DHS Directives and policy, via the Component Chief Information Officer.

D. The ***Component Chief Information Officers*** establish, oversee, and implement the Component's IT Security Program.

E. The ***Chief Privacy Officer*** establishes, oversees the implementation of, and issues guidance on DHS privacy policy (See DHS Directive 047-01, "Privacy Policy and Compliance").

F. The ***Chief Financial Officer***:

1. Designates financial systems and oversees security control definitions for financial systems (See DHS Directive 252-10, "Financial Management Line of Business Integration and Management"); and

2. Implements and manages the DHS Financial Program, including oversight of DHS financial systems.

G. The ***Chief Security Officer***

1. Implements and manages the DHS Security Program for DHS facilities and personnel (See DHS Directive 121-01, "Chief Security Officer"); and

2. Implements Foreign Access Management protocols for foreign access affecting DHS IT [See DHS Directive 121-08, "Requirements for Security Review of Foreign National Assignments and Overseas Employment"].

H. The ***DHS Chief Information Security Officer (CISO)***:

1. Implements and maintains a Federal Information Security Modernization Act (FISMA) compliant IT Security Program;

2. Chairs the DHS CISO Council; and

3. Oversees compliance with "DHS Sensitive Systems Policy 4300A" and "DHS National Security Systems Policy 4300B."

I. The ***DHS CISO Council*** coordinates and provides input on DHS CISO IT policies and initiatives.

J. The ***Component Chief Information Security Officers*** and/or ***Information System Security Managers*** ensure compliance with the Departmental IT security Directives and policies.

V. Policy and Requirements

A. The DHS IT Security Program:

1. Establishes Department-wide programmatic requirements to ensure a secure network security infrastructure and operations that integrate confidentiality, availability, and integrity into the infrastructure design, implementation, and maintenance in order to:

a. Protect the Department's infrastructure and critical information assets from internal and external threats arising from connections to the DHS network and Internet.

b. Ensure that IT resources attached to the DHS network are consistent with, and supportive of, a secure network IT infrastructure design.

c. Protect DHS IT resources from malicious threats or unauthorized use, as well as unintentional misuse by authorized persons.

d. Maintain the appropriate level of security to support the ability of the Department to conduct its work.

2. Provides the requirements for DHS Components to use in establishing IT Security Programs.

3. Ensures comprehensive, uniform IT security policies throughout the Department by managing the implementation of "DHS Sensitive Systems Policy 4300A" and "DHS National Security Systems Policy 4300B".

4. Requires:

a. Periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the Department;

b. Annual security and privacy awareness training for all DHS personnel;

c. Periodic testing and evaluation of the effectiveness of security controls based on risk to include, at a minimum, certification testing of appropriate management, operational, and technical controls;

d. A process for planning, developing, implementing, evaluating, and documenting remedial actions to address deficiencies in information security policies, procedures, and practices;

e. A process for continuity of operations for information systems that support the operations and assets of the Department; and

f. Procedures for detecting, immediately reporting, and responding to security incidents.

B. All DHS Components follow DHS Directives and policies, guidelines, and other IT Security Program Publications. These policies and publications are available online, and are reviewed pursuant to DHS Directive 112-01, "The Directives System."

VI. Questions

Address any questions or concerns regarding this Directive to the Office of the Chief Information Officer, Office of the Chief Information Security Officer, infosecpolicy@hq.dhs.gov.

MAY 0 5 2017

Chip Fulghum
Acting Under Secretary for Management

Date