

INFORMATION TECHNOLOGY SECURITY PROGRAM

I. Purpose

This Directive establishes Department of Homeland Security (DHS) policy regarding the Information Technology (IT) Security Program. This Directive assigns the responsibilities for the integration and management of the IT Security Program's policies, methodologies, tools, and reviews.

II. Scope

- A. This Directive applies throughout DHS, to all IT systems, including National Security systems.
- B. The authority of the:
 - 1. Inspector General as set forth in the Inspector General Act is not reduced by provisions within this Directive.
 - 2. Under Secretary for Intelligence and Analysis (I&A) concerning intelligence activities are not affected by this Directive.
- 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.
- D. This cancels and supersedes the Addendum C, "DHS Information Technology Security Program," within Management Directive 0007.1, "Information Technology Integration and Management."

III. Authorities

- A. Public Law 107-347, "The E-Government Act of 2002"
- B. Title 5, United States Code (U.S.C.), Section 552a, "Records Maintained On Individuals"
- C. Title 44, U.S.C., Chapter 35, "Coordination of Federal Information Policy"

- D. E.O. 13231, "Critical Infrastructure Protection in the Information Age"
- E. Title 5, Code of Federal Regulations (CFR), Section 2635, "Office of Government Ethics, Standards of Ethical Conduct for Employees of the Executive Branch"
- F. Presidential Decision Directive 63, "Critical Infrastructure Protection"
- G. Office of Management and Budget (OMB) Circular A-123, "Management's Responsibility for Internal Control"
- H. OMB Circular A-130, "Management of Federal Information Resources"
- I. DHS Delegation 04000, "Delegation for Information Technology"

IV. Responsibilities

- A. The **DHS Chief Information Officer (CIO)**:
 - 1. Oversees the 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 Information Security Program annually;
 - 4. Provides feedback to the Component Chief Information Officers on the evaluation of the DHS Information Security Program;
 - 5. Participates in the development of the DHS performance plans, including descriptions of the time periods and budget, staffing, and training resources required to implement the Department-wide Information Security Program;
 - 6. Establishes information security procedures, including supporting governance structures and consistent with the policies contained within this Directive;
 - 7. Ensures continuity of operations by participating in continuity planning; and
 - 8. Leads the DHS Contingency Planning Program.

- B. The **Component heads** ensure that an IT Security Program is implemented within their Components in accordance with this Directive.
- C. The **Component Chief Information Officers** establish, oversee, and implement the Component's Information Security Program.
- D. The **DHS Chief Information Security Officer (CISO)**:
1. Implements and maintains a Federal Information Security Management Act (FISMA) compliant Information Security Program;
 2. Defines FISMA compliance and oversight requirements and performance metrics;
 3. Establishes qualifications for information security positions within the Department;
 4. Monitors Component information security training programs and establishes standards for compliance with Departmental requirements;
 5. Supports established IT Security Governance processes and provides recommendations to the DHS CIO;
 6. Provides input and feedback to the Component Chief Information Security Officers regarding issues that affect the Components;
 7. Chairs the DHS CISO Council; and
 8. Exercises the oversight responsibilities for the enterprise security operation functions.
- E. The **DHS CISO Council** coordinates and provides input on major DHS CISO information security policies and initiatives.
- F. The **Component Chief Information Security Officers** and/or **Information System Security Managers**:
1. Ensure compliance with the Departmental information security policies;
 2. Ensure that information security decisions are distributed to the Information System Security Officer (ISSO) and other appropriate officials;
 3. Apprise the Component Chief Information Officer of all pertinent matters involving the security of IT systems; and

4. Appoint ISSOs as required.

V. Policy and Requirements


- A. The DHS CISO implements the DHS Information Security Program as directed by the DHS CIO.
- B. The DHS CISO ensures the timely dissemination of effective security.
- C. The DHS IT Security Program serves as a foundation for DHS Components to use in establishing IT Security Programs. The IT Security Program ensures comprehensive, uniform IT security policies are followed by each DHS Component.
- D. The DHS Information Security Program includes the following fundamentals:
 1. 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.
 2. Selection and effective implementation (through Component Security Programs) of minimum, mandatory technical, operational, and management security controls, or other compensating countermeasures, to protect the confidentiality, integrity, and availability of each Department system and its information.
 3. Annual security awareness training for all DHS employees.
 4. 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.
 5. A process for planning, developing, implementing, evaluating, and documenting remedial actions to address deficiencies in information security policies, procedures, and practices.
 6. Procedures for detecting, immediately reporting, and responding to security incidents.
- E. The DHS CISO establishes and manages a process for in depth review of all DHS operational systems.
- F. The DHS CISO provides the DHS CIO and Department leadership with an

evaluation of the Departmental and Component information security posture.

G. All DHS Components follow guidelines and policies as outlined herein and in the IT Security Program Publications. These policies and publications are available online, after review by the Office of the Under Secretary for Management, Office of the General Counsel, Privacy Office, and Component Chief Information Security Officers and approval by the DHS CISO.

VI. Questions

Address any questions or concerns regarding this Directive to the Office of the Chief Information Officer.


Chris Cummiskey
Acting Under Secretary for Management

7/6/14
Date