

DHS INFORMATION SHARING ENVIRONMENT TECHNOLOGY PROGRAM

I. Purpose

This Directive establishes the Department of Homeland Security (DHS) information technology (IT) program for the DHS Information Sharing Environment (DHS ISE).

II. Scope

This Directive applies throughout DHS, unless exempted by statutory authority.

III. Authorities

- A. Title 6, United States Code (U.S.C.), Chapter 1, "Homeland Security Organization," Sections 121, 124b, 482, and 485
- B. Title 40, U.S.C., Subtitle III, "Information Technology Management," Sections 11101, 11315, and 11316
- C. Title 44, U.S.C., Chapter 35, "Coordination of Federal Information Policy" and Chapter 36, "Management and Promotion of Electronic Government Services"
- D. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources"
- E. DHS Memorandum from Secretary Michael Chertoff, "Information Sharing at the Department of Homeland Security," December 16, 2005
- F. DHS Memorandum, "DHS Policy for Internal Information Exchange and Sharing," February 1, 2007
- G. DHS Memorandum, "Federal Information Sharing Environment Privacy and Civil Liberties Policy," June 5, 2009
- H. DHS Delegation 00002, "Delegation to the Under Secretary for Management"
- I. DHS Delegation 04000, "Delegation for Information Technology"

- J. DHS Delegation 08503, “Delegation to the Under Secretary for Intelligence and Analysis/Chief Intelligence Officer”
- K. DHS Sensitive Systems Policy Directive 4300A
- L. DHS Directive 262-05, “Information Sharing and Safeguarding”

IV. Responsibilities

A. The **DHS Information Sharing and Safeguarding Governance Board (ISSGB)**:

1. Develops and oversees the implementation of the DHS information sharing and safeguarding strategy;
2. Provides oversight and governance of Department-wide initiatives relating to information sharing and safeguarding;
3. Establishes goals and priorities relating to information sharing and safeguarding; and
4. Ensures consistency in information sharing and safeguarding policy and procedures both within the Department and between the Department and other Federal agencies, Tribal, State, territorial, local governments, private sector, and international partners.

B. The **Under Secretary for Intelligence and Analysis (I&A)**:

1. Serves as the Senior Information Sharing and Safeguarding Executive for the Department, exercising leadership, in conjunction with and without preempting the authorities of the DHS Chief Information Officer and DHS Chief Security Officer, over information sharing and safeguarding policy and programs throughout the Department in partnership with the other Component heads, advising and assisting the Secretary, Deputy Secretary, Component heads, and other senior officials in carrying out the Department’s responsibilities for information sharing and safeguarding;
2. Communicates and implements the Secretary’s leadership direction related to the information sharing and safeguarding function of the Department; and
3. Serves as the Chair and Executive Agent of the ISSGB.

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

1. Supervises the management of the Information Technology (IT) priorities for the DHS ISE, as administered by the Information Sharing Environment Office (ISEO);
2. Ensures efficient and effective use of resources by establishing unified policies and business processes, and the use of shared or centralized services and standards and automated solutions, for the purpose of achieving functional excellence in support of the Department's missions and objectives, including with respect to IT policies and processes concerning the DHS ISE;
3. Serves as the Vice-Chair of the ISSGB;
4. Selects and oversees technological solutions that enable seamless information sharing throughout the Department;
5. Serves as the executive agent for the ISE's IT portfolio, composed of systems, initiatives, and programs;
6. In conjunction with the **Under Secretary for I&A**:
 - a. Defines the information sharing and safeguarding architecture for the Department and between DHS and other departments' and agencies' information sharing and safeguarding architectures;
 - b. Leads various technology related initiatives within the Department, Federal agencies, and non-Federal entities related to the IT deployment of the ISE across the Homeland Security Enterprise;
 - c. Provides resources as well as management and oversight of the Information Sharing Equipment Coordination Activity; and
 - d. Provides oversight and management of the DHS Suspicious Activity Reporting Technology Initiative.
7. Works with Component heads through their respective Chief Information Officers, determining technical and system security designs for their information needs and priorities;
8. Provides technical oversight, architecture development, and policy guidance supporting the implementation of Federal Identity Credential and Access Management, to include federated identity management across the DHS ISE;

9. Provides technical oversight and management of the Homeland Security Information Network in conjunction with the Office of Operations Coordination and Planning; and

10. Serves as the DHS representative to the National Information Exchange Model (NIEM) Executive Steering Council and provides resources to support the NIEM Program as described in the Memorandum of Understanding between the Department of Justice and DHS.

D. The **Component heads:**

1. Ensure compliance with this Directive, through the Component Chief Information Officer;

2. Provide oversight for the evaluation of IT investments by evaluating information sharing and safeguarding opportunities; and

3. Ensure appropriate information sharing is reflected in Component policies and functional requirements.

E. The **Component Chief Information Officers:**

1. Ensure the Component complies with and effectively implements the policies and responsibilities in this Directive;

2. Provide advice to their Component heads, ensuring that information sharing IT resources are acquired, used, and managed within the Component efficiently; and

3. Promote appropriate information sharing as described in “DHS Policy for Internal Information Exchange and Sharing,” and “The Department of Homeland Security’s Federal Information Sharing Environment Privacy and Civil Liberties Policy.”

F. The **DHS Chief Privacy Officer:**

1. Ensures activities under this Directive incorporate privacy protections by implementing the Fair Information Practice Principles, and by recommending to the Secretary ways to minimize or mitigate any potential risks to individual privacy; and

2. Serves as the Department’s ISE Privacy Official.

G. The **Officer for Civil Rights and Civil Liberties:**

1. Ensure activities under this Directive incorporates civil rights and civil liberties protections, and recommends to the Secretary ways to minimize or mitigate any potential risks to individual liberties; and

2. Serves as the Department's ISE Civil Liberties Official.

V. Policy and Requirements

A. Information is a strategic asset to DHS, which is appropriately safeguarded and the information is made available throughout the information life cycle to any DHS user or mission partner consistent with applicable statute, executive order, presidential or other directive, regulation, international obligation, or national or departmental policy.

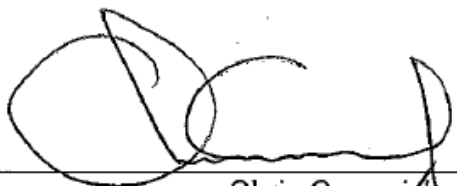
B. It is the policy of the Department to appropriately collect, use, retain, and disseminate information that is safeguarded, discoverable, retrievable, accurate, relevant, timely, and actionable to improve mission operations. The data collected, used, retained, and disseminated is done so in compliance with the DHS enterprise data architecture.

C. In accordance with enterprise data policy and guidance, including protections for civil rights and civil liberties, Components, to the greatest extent possible, share their information in compliance with standardized data structures and tag information for appropriate access.

D. To the greatest extent possible, Component heads integrate national and departmental policies, technologies, investments, procedures, and performance measures when interacting with mission partners.

VI. Questions

Address any questions or concerns regarding this Directive to the Office of the Chief Information Officer (OCIO), Information Sharing Environment Office (ISEO).


Chris Cumiskey
Acting Under Secretary for Management

10/10/14
Date