

## INFORMATION SHARING AND SAFEGUARDING

---

### I. Purpose

This Directive establishes the policy and governance framework for information sharing and safeguarding both within the Department and between the Department and its Federal, State, local, tribal, territorial, private sector, and international partners.

### II. Scope

This Directive applies throughout the Department. Aspects of this Directive may apply to routine information sharing engagements, but nothing in this Directive is intended to impede the authorized conduct of those engagements by any departmental official or entity, and nothing in this directive prohibits the sharing of information in exigent circumstances consistent with applicable statute, executive order, presidential or other directive, regulation, international or domestic agreement, arrangement, or obligation, and national and departmental policy.

### III. Authorities

- A. Title 5, United States Code, Section 552a, "Privacy Act of 1974," as amended
- B. Public Law No. 107-296, "Homeland Security Act of 2002," as amended
- C. Public Law No. 108-458, "Intelligence Reform and Terrorism Prevention Act of 2004," as amended
- D. DHS Delegation No. 08503, "Delegation to the Under Secretary for Intelligence and Analysis/Chief Intelligence Officer," August 10, 2012

### IV. Responsibilities

- A. The **Under Secretary for Intelligence and Analysis (USIA)** serves as the Chief Intelligence Officer and Senior Information Sharing and Safeguarding Executive for the Department. The USIA exercises leadership and authority in conjunction with and without preempting the authorities of the Department of Homeland Security (DHS) Chief Information Officer, the DHS Chief Security Officer, and the Heads of

other Components, as appropriate over information sharing and safeguarding policy and programs throughout the Department. As the Chair of the Information Sharing and Safeguarding Governance Board, the USIA advises and assists the Secretary, Deputy Secretary, Component Heads, and other senior officials in carrying out DHS's responsibilities for information sharing and safeguarding and communicates the Secretary's leadership direction in this area and manages the execution of this Directive.

- B. The **DHS Chief Information Officer (CIO)** is responsible for the approval, management and oversight of the Department's Information Technology (IT) programs, ensuring 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.
- C. The **DHS Chief Security Officer (CSO)** is responsible for the supervision, oversight, and direction of the Department's security program for personnel security, information security, administrative security, classification management of national security information, physical security, operations security, industrial security, security training and awareness, and the Personal Identity Verification (PIV) card program.
- C. The **Under Secretary for National Protection and Programs** is responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department, including the operation of the National Infrastructure Coordination Center and the National Cybersecurity and Communications Integration Center to serve as Federal Government focal points for critical infrastructure security and resilience-related information sharing, including but not limited to sharing with critical infrastructure partners, and to provide a situational awareness capability and integrated, actionable information about emerging trends, imminent threats, and the status of incidents that impact critical infrastructure.
- D. The **Assistant Secretary for Policy** is responsible for ensuring, in coordination with the Components, that information sharing and safeguarding activities comply with applicable Department-wide policies, programs, strategies, and plans.
- E. The **Assistant Secretary for International Affairs** serves as the principal international advisor to the Office of the Secretary and other leadership of the Department, maintaining situational awareness of and coordinating DHS relations with foreign governments, international organizations, and international non-governmental organizations, including entering into international agreements and arrangements.

- F. The **General Counsel**, the **Chief Privacy Officer**, and the **Officer for Civil Rights and Civil Liberties** ensure that departmental information sharing and safeguarding activities comply with applicable law and adequately protect individuals' privacy and civil rights and civil liberties, respectively.
  
- G. The **Heads of All Components** implement and execute all applicable policies and procedures set forth in this Directive and any implementing instructions or other policy guidance to the extent permitted by and consistent with those Component Heads' authorities and any restrictions imposed by statute, executive order, presidential or other directive, or national or departmental policy.

## V. Policy and Requirements

### A. **Policy:**

1. **DHS Information Sharing Environment (DHS-ISE):** The primary policy and technology framework for the sharing and safeguarding of terrorism information, homeland security information, and homeland security-relevant information within the Department is the DHS Information Sharing Environment (DHS-ISE), which consists of the mission processes and supporting core capabilities that facilitate information sharing and safeguarding both within the Department and between the Department and external entities.
  - a. On behalf of the Secretary, the DHS Information Sharing and Safeguarding Governance Board (ISSGB) governs the DHS-ISE.
    - i. The ISSGB sets broad guidelines and general policies with the intention of facilitating and enabling efficient and effective information sharing and safeguarding across the Department. It develops and oversees the implementation of the DHS Information Sharing and Safeguarding Strategy; establishes, implements, and oversees processes and guidelines for addressing information sharing and safeguarding gaps and the identification, analysis and mitigation of risk concerning information sharing and safeguarding; serves as a steering committee and decision-making body for DHS collaboration on information sharing and safeguarding issues; provides policy guidance concerning the sharing and safeguarding of terrorism information, homeland security information, and homeland security-relevant information; establishes goals and priorities relating to information sharing and safeguarding; provides recommended programmatic guidance for departmental

information sharing and safeguarding initiatives; establishes and oversees additional subordinate councils, executive steering committees, integrated project teams and working groups responds to reporting requirements of the ISE concerning the DHS-ISE; and provides training and guidance to employees, officials, and senior executives within the Department concerning the DHS-ISE, as appropriate.

ii. The ISSGB does not direct or oversee the day-to-day operations of Components or elements thereof; rather, the ISSGB leverages departmental resources and synchronizes departmental policies and processes to ensure that priority initiatives pertaining to information management are supported across the Department.

b. The USIA is the Chair and Executive Agent of the ISSGB, issuing instructions, processes, standards, guidelines, procedures, strategies, or other policy guidance on behalf of the ISSGB with the approval of the ISSGB. The CIO is the Vice-Chair of the ISSGB.

2. **Information Sharing Environment Activities:** In addition to the governance generally provided by the ISSGB and its subordinate governance bodies with respect to the DHS-ISE, the Department's efforts to address insider threats is coordinated through the Insider Threat Program led by the USIA in coordination with the CIO and the CSO, its engagement with and support to State and Major Urban Area Fusion Centers is coordinated through the DHS State, Local, and Regional Fusion Center Initiative led by the USIA, and its support for and engagement with the Nationwide SAR Initiative (NSI) is led by the USIA.

3. **One DHS Rule:** For information sharing and safeguarding purposes, including for purposes of Title 5, United States Code, Section 552a, "Privacy Act of 1974," the Department is one agency, and no Component is a separate agency from another Component.

B. **Requirements:**

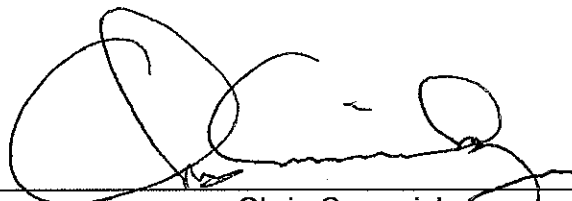
1. **Internal Access to Departmental Information:** In accordance with the One DHS Rule, Components share information as one Department, rather than as separate entities to the extent permitted by and consistent with those Component Heads' authorities and any restrictions imposed by statute, executive order, presidential or other directive, or national or departmental policy. The ISSGB, in coordination with affected Component Heads or their designees,

promulgates policies, processes, standards, and guidelines implementing this requirement.

2. **Information Sharing and Access Agreements:** The ISSGB, in coordination with affected Component Heads or their designees, promulgates policies, processes, standards, and guidelines pertaining to Information Sharing and Access Agreements (ISAAAs). Where appropriate, the ISSGB reviews ISAAAs to determine whether an exception to the One DHS Rule is warranted, but it does not otherwise review individual ISAAAs.
3. **Technology Alignment:** To the greatest extent feasible, Components standardize the technology used to categorize, access, exchange, and manage information in automated systems to permit the effective location and use of the most current and complete data available in support of the Department's missions and align their IT architecture with the Homeland Security Enterprise Architecture approved by the ISSGB.

## VI. Questions

Address any questions or concerns regarding this Directive to the Office of Intelligence and Analysis.

 9/4/14  
\_\_\_\_\_  
Chris Cumiskey  
Acting Under Secretary for Management

\_\_\_\_\_  
Date