



Homeland Security

U.S. Department of Homeland Security
Office of Intelligence and Analysis
Homeland Security Information Sharing Procedures: 2015-01

HOMELAND SECURITY INFORMATION SHARING PROCEDURES

I. Purpose

This directive implements Title 6, United States Code (U.S.C.), Section 482, and dictates the manner in which federal agencies share homeland security information, as defined herein, with other federal agencies and appropriate state and local personnel.

II. Scope

This directive applies to all agencies of the federal government. The President may make, or may authorize another officer of the United States to make, exceptions to this directive. Nothing in this directive is intended to require or should be interpreted as requiring violation of the Constitution or other existing law, executive order, presidential or other directive, regulation, international obligation, national or departmental policy, or an existing information sharing agreement or arrangement. Nothing in this Directive is intended to abrogate or interfere with the authorities or responsibilities of any federal department or agency, including their authorities and responsibilities to engage in information sharing activities or agreements with federal, state, local, tribal, territorial, international, and private sector entities.

This directive is intended to improve the internal management of the federal government and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

III. Authorities

- A. The Homeland Security Act of 2002, Public Law 107-296, as amended, section 892, "Facilitating Homeland Security Information Sharing Procedures."
- B. The Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, as amended, section 1016, "Information Sharing."
- C. Executive Order (E.O.) 13,311, "Homeland Security Information Sharing," July 29, 2003.
- D. E.O. 13,526, "Classified National Security Information," December 29, 2009.

- E. DHS Delegation 08503, "Delegation to the Under Secretary for Intelligence and Analysis/Chief Intelligence Officer," August 10, 2012.

IV. Definitions

- A. **Classified Information** or **Classified National Security Information**: Information that has been determined pursuant to E.O. 13,526 or any predecessor executive order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.
- B. **Homeland Security Information**: Any information possessed by a federal, state, or local agency that (1) relates to the threat of terrorist activity; (2) relates to the ability to prevent, interdict, or disrupt terrorist activity; (3) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (4) would improve the response to a terrorist act.
- C. **Information Sharing Environment (ISE)**: A national approach that facilitates the sharing of terrorism information and homeland security information.
- D. **Intelligence Community**: Certain designated federal government agencies, services, bureaus, or other organizations that play a role in the gathering or use of national intelligence, as defined at Title 50, U.S.C., Section 3003(4), "Definitions," and E.O. 12,333, "United States Intelligence Activities," Section 3.5(h), as amended.
- E. **Sensitive But Unclassified Information**: Information that is not classified information, but is sensitive in nature, and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of federal programs, or other programs or operations essential to the national interest.
- F. **State**: The term "State" includes the District of Columbia and any commonwealth, territory, or possession of the United States.
- G. **State and local personnel**: Any of the following persons involved in prevention, preparation, or response for terrorist attack: (1) state governors, mayors, and other locally elected officials; (2) state and local law enforcement personnel and firefighters; (3) public health and medical professionals; (4) regional, state, and local emergency management agency personnel, including state adjutant generals; (5) other appropriate emergency response agency personnel; and (6) employees of private-sector entities that affect critical infrastructure, cyber, economic, or public health or security, as designated by the heads of Agencies.
- H. **Terrorism** or **Terrorist Activity**: Any activity that (1) involves an act that (a) is dangerous to human life or potentially destructive of critical infrastructure and (b) is a violation of the criminal laws of the United States or of any state or other subdivision of the United States; and (2) appears to be intended (a) to intimidate or coerce a civilian population, (b) to influence the policy of a

government by intimidation or coercion, or (c) to affect the conduct of a government by mass destruction, assassination, or kidnapping.

- I. **Terrorism Information**: All information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to (1) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (2) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; (3) communications of or by such groups or individuals; or (4) groups or individuals reasonably believed to be assisting or associated with such groups or individuals. The term includes weapons of mass destruction information.
- J. ~~(U//FOUO)~~ **Weapons of Mass Destruction Information**: Information that could reasonably be expected to assist in the development, proliferation, or use of a weapon of mass destruction (including a chemical, biological, radiological, or nuclear weapon) that could be used by a terrorist or a terrorist organization against the United States, including information about the location of any stockpile of nuclear materials that could be exploited for use in such a weapon that could be used by a terrorist or a terrorist organization against the United States.

V. Responsibilities

- A. The **Under Secretary of Homeland Security for Intelligence and Analysis** prescribes and implements, in coordination and consultation with the heads of affected federal departments and agencies, procedures under which federal agencies (1) share relevant and appropriate homeland security information with other federal departments and agencies, and appropriate state and local personnel; (2) identify and safeguard homeland security information that is sensitive but unclassified; and (3) to the extent such information is in classified form, determine whether, how, and to what extent to remove classified information, as appropriate, and with which such personnel it may be shared after such information is removed.
- B. The **Program Manager of the Information Sharing Environment**, consistent with the direction and policies issued by the President, the Director of National Intelligence, and the Director of the Office of Management and Budget, issues government-wide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE.
- C. The **Heads of Federal Departments and Agencies** 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 heads' authorities and any restrictions imposed by the

Constitution, statute, executive order, regulation, presidential or other directive, or national or departmental policy. The heads of federal departments and agencies affected by this Directive designate an official to administer this Directive with respect to their department or agency.

VI. Policy and Requirements

A. Policy:

1. The federal government is required by the Constitution to provide for the common defense, which includes deterring, preventing, and preempting a terrorist attack, and it relies on state and local personnel to assist in protecting against a terrorist attack. State and local personnel have capabilities and opportunities to gather information on suspicious activities and terrorist threats not possessed by federal agencies, and the federal government and state and local governments and agencies in other jurisdictions may benefit from such information. The needs of state and local personnel to have access to relevant homeland security information to combat terrorism is balanced against the need to preserve the protected status of such information and to protect the sources and methods used to acquire such information. Federal, state, and local governments and intelligence, law enforcement, and other emergency preparation and response agencies must act in partnership to maximize the benefits of information gathering and analysis to prevent and respond to terrorist attacks. Information sharing systems have been established for rapid sharing of classified and sensitive but unclassified information among federal, state, and local entities. These systems include, but are not limited to, the International Justice and Public Safety Network, the National Terrorism Advisory System, the Homeland Security Information Network, and the Homeland Secure Data Network.
2. Federal agencies share homeland security information through information sharing systems, including homeland security information that is classified or otherwise sensitive but unclassified, together with assessments of the credibility of such information with other federal departments and agencies as well as appropriate state and local personnel in accordance with policies, procedures, guidelines, rules, and standards that govern the content and usage of the ISE, to the extent required by section 1016(i) of the Intelligence Reform and Terrorism Prevention Act of 2004.
3. Federal agencies share homeland security information in accordance with the Constitution, relevant federal laws, Executive Orders, department and agency regulations, policies and procedures, and applicable judicial minimization procedures and handling requirements.
4. Under Title 6 U.S.C., Section 482(e), homeland security information obtained by a state or local government from a federal department or agency under this directive remains under the control of the federal

department or agency, and a state or local law authorizing or requiring such a government to disclose information does not apply to such information.

B. **Requirements:**

1. The heads of federal departments and agencies ensure that information sharing systems used by their departments or agencies to share homeland security information possess the following capabilities: (a) the capability to transmit unclassified or classified information, even if the procedures for each capability differ; (b) the capability to restrict delivery of information to specified subgroups by geographic location, type of organization, position of a recipient within an organization, or a recipient's need to know such information; (c) a configuration that allows for the efficient and effective sharing of information; and, (d) accessibility to appropriate state and local personnel.
2. The heads of federal departments and agencies ensure that information sharing systems used by their departments or agencies to share homeland security information, to the extent reasonably practicable and consistent with section VI.A of this directive, (a) limit the re-dissemination of homeland security information to ensure that such information is not used for an unauthorized purpose; (b) ensure the security and confidentiality of such information; (c) protect the constitutional and statutory rights of any individuals who are subjects of the homeland security information; and (d) provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.
3. Federal departments and agencies identify and share homeland security information, as described in section VI of this Directive, in a manner that is consistent with all laws, regulations, and policies related to the sharing and safeguarding of classified information and sensitive but unclassified information, the protection of intelligence sources and methods, and the protection of privacy, civil rights, and civil liberties.

VII. Questions

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

(b) (6)

Francis X. Taylor

Under Secretary for Intelligence and Analysis
U.S. Department of Homeland Security

April 15, 2016
Date