

**U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT**  
**ICE Policy System**

**OFFICE OF PRIMARY INTEREST: OFFICE OF INVESTIGATIONS**

<b>DISTRIBUTION:</b>	ICE
<b>DIRECTIVE NO.:</b>	5-2.0
<b>ISSUE DATE:</b>	March 23, 2007
<b>EFFECTIVE DATE:</b>	March 23, 2007
<b>REVIEW DATE:</b>	March 23, 2010
<b>SUPERSEDES:</b>	None

**DIRECTIVE TITLE: SAFEGUARDING LAW ENFORCEMENT SENSITIVE INFORMATION**

1. **PURPOSE and SCOPE.** This Directive establishes U.S. Immigration and Customs Enforcement (ICE) policy and procedures for the identification of law enforcement sensitive (LES) information and the measures that are required to safeguard it. This includes policy and procedures related to the dissemination of LES information outside the Department of Homeland Security (DHS). It is a DHS priority to ensure appropriate access to and sharing, integration, and use of information by federal, state, local, and foreign agencies with law enforcement and counterterrorism responsibilities and, as appropriate, with private sector entities.
2. **AUTHORITIES/REFERENCES.**
  - 2.1 DHS Management Directive (MD) 11042.1, "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated January 6, 2005.
  - 2.2 DHS Memorandum to Secretary Chertoff, "Information Sharing at the Department of Homeland Security," dated December 16, 2005, and approved March 21, 2006.
  - 2.3 DHS MD 0450.1, entitled, "Memoranda of Understanding (MOU) and Memoranda of Agreement (MOA)," issued January 24, 2003.
  - 2.4 5 U.S.C. § 552, The Freedom of Information Act, as amended by Public Law No. 104-231. 110Stat. 3048.
  - 2.5 5 U.S.C. § 552a, The Privacy Act.
  - 2.6 ICE Information Technology (IT) Security Manual for Sensitive Systems.

---

ICE Directive: Safeguarding Law Enforcement Sensitive Information

- 2.7 DHS MD 4300.1, "Information Technology Systems Security."
- 2.8 DHS Publication 4300A, entitled "DHS Sensitive Systems Policy" (Version 4.0), issued June 1, 2006.
- 2.9 DHS Publication 4300A, entitled "Sensitive Systems Handbook" (Version 4.0), issued June 1, 2006.
- 2.10 Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," October 25, 2005.

**3. SUPERSEDED/CANCELLED POLICY/SUMMARY OF CHANGES.**  
None.

**4. BACKGROUND.**

- 4.1 ICE is governed by policy articulated in DHS MD 11042.1 for the identification and safeguarding of sensitive but unclassified (SBU) information originated within DHS and other SBU information received by DHS from other government and non-government entities.
- 4.2 Under DHS policy, "FOR OFFICIAL USE ONLY" (FOUO) is used within DHS to identify SBU information that is not otherwise specifically described and governed by statute or regulation. DHS MD 11042.1 acknowledges that some types of SBU information, including law enforcement information, may be more sensitive than others and warrant additional identification and safeguarding measures beyond the minimum requirements established by DHS policy.
- 4.3 In recognition of the unique nature of law enforcement information, ICE further identifies law-enforcement-related SBU information as LES.
- 4.4 SBU information that is LES is marked as FOUO and LES in order to control and restrict access to that information. The loss, misuse, or unauthorized access to such information could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. § 552a (the Privacy Act). The loss, misuse, or unauthorized access to such information could also cause the obstruction or impairment of official law enforcement or regulatory functions; damage leading to loss of life or personal injury; loss of property through fraud, theft, or other unlawful means; loss of privacy of an individual; gain by an individual, corporation, or any other type of commercial business structure of an unfair advantage in the competitive marketplace; or damage to a person or any type of commercial business structure that has entrusted its proprietary information to the U.S. Government.

5. **DEFINITIONS.** The following definitions are provided for the purposes of this Directive:
- 5.1 **Authorized:** Determination made by an ICE official that access to ICE LES information is sanctioned by DHS and ICE policies or directives.
- 5.2 **For Official Use Only (FOUO):** Term used within DHS to identify information that is FOUO, which is unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, 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. Information impacting the national security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 12958, "Classified National Security Information," as amended, or its predecessor or successor orders, is not to be considered FOUO. FOUO information is not to be considered classified information.
- 5.3 **Law Enforcement Sensitive (LES):** Term used within ICE to identify LES information. LES information is a type of FOUO information that is compiled for law enforcement purposes, the unauthorized disclosure of which could adversely impact the conduct of law enforcement programs or the privacy or welfare of involved persons. Information impacting the national security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 12958, "Classified National Security Information," as amended, or its predecessor or successor orders, is not to be considered FOUO/LES. If LES information is classified, it is no longer subject to the provisions of this Directive.
- 5.4 **Need-to-Know:** Determination made by the originator that a prospective recipient requires access to specific information in order to perform or assist in a lawful and authorized government function.
- 5.5 **Open Investigation:** ICE investigation for which not all leads have been exhausted or that has not been fully adjudicated, and which has been assigned a status of "open" in the investigation case management system of records. The status of an investigation is determined by the investigator or supervisory or management official having program management responsibility over the investigation.
- 5.6 **Originator:** ICE employee, detailee, or contractor who prepares material that contains information designated as LES per section 5.3 of this Directive. A supervisor or management official may act on behalf of the originator.
- 5.7 **Originating Office:** The Program Office where the originator works, including the originator's supervisor, Principal Field Officer or Principal Headquarters Officer, and Program Office Director.

**5.8 Terrorism Information:** Information defined as “terrorism information” in 6 U.S.C. § 485(a)(4) and Executive Order 13388 where such information is not classified. “Terrorism information” means 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 to 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; and
- 4) Groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

## **6. POLICY.**

### **6.1 Designation of Information as Law Enforcement Sensitive.**

- 1) ICE defines FOUO information as LES when any unauthorized release could fall within the categories defined by the Freedom of Information Act exemption 7, which applies to information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records of information:
  - a. Could reasonably be expected to interfere with law enforcement proceedings or investigations;
  - b. Would deprive a person of a right to a fair trial or an impartial adjudication;
  - c. Could reasonably be expected to constitute an unwarranted invasion of personal privacy;
  - d. Could reasonably be expected to disclose the identity of a confidential source, including a state, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, or, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source;



- e. Would disclose techniques and procedures for law enforcement investigations or prosecutions, guidelines for law enforcement investigations or prosecutions, or the location and number of assets if such disclosure could reasonably be expected to risk circumvention of the law; or
  - f. Could reasonably be expected to endanger the life or physical safety of any individual.
- 2) Any ICE employee, detailee, or contractor, in the course of performing assigned duties, shall designate information falling within one or more of the categories cited in section 6.1(1) of this Directive as LES.
  - 3) The removal of the LES designation may be carried out either by the originating office or through the normal process of clearance for public release.
  - 4) Information designated as LES will retain its designation until determined otherwise by the originator or the originating office.

## **6.2 Marking Law Enforcement Sensitive Information.**

- 1) Materials containing FOUO/LES information generated by ICE may be marked "LAW ENFORCEMENT SENSITIVE" in addition to the DHS FOUO marking defined in DHS MD 11042.1. Where the sensitivity of the information warrants additional access and dissemination restrictions, the originator may cite restrictions such as the following:

*WARNING: This document has been designated DHS Law Enforcement Sensitive and is to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS and ICE policy relating to Law Enforcement Sensitive information. This information can be distributed further within DHS on a need-to-know basis; however, it may not be distributed outside DHS without authorization from the originating office.*

- 2) Materials containing specific types of LES information may be further marked with an applicable marking in order to alert the reader of the type of information the materials contain. Where the sensitivity of the information warrants restricted access and dissemination, the originator may cite applicable restrictions, including, but not limited to, the following:

- a. **Grand Jury Material** – Used in accordance with Federal Rule of Criminal Procedure 7(e), only in the case of sharing to assist in prosecution in accordance with rule 6(e)(3)(A);
  - b. **Child Victim/Witness** – Protect identity in accordance with 18 U.S.C. § 3509;
  - c. **Juvenile** – Protect identity in accordance with 18 U.S.C. § 5031;
  - d. **Witness Security Program** – Protect identity in accordance with 18 U.S.C. § 3521;
  - e. **Restricted by Court Order** – Rules depend on the text of the Court Order;
  - f. **Proprietary** – Used in accordance with 18 U.S.C. § 1905, or in accordance with written agreement between ICE and the provider of the information;
  - g. **Federal Taxpayer Information** – Used when information is shared with ICE by the Internal Revenue Service in accordance with 26 U.S.C. § 6103;
  - h. **Deliberative Process** – The processes of evaluating relevant evidence, arguments, and options, for the purpose of making a decision related to the performance of an agency's functions; or
  - i. **Not to be Disclosed Outside of Internal DHS Intelligence Channels** – Used when information is requested by DHS under the DHS Intelligence and Analysis (I&A) Request for Information (RFI) program, or when I&A requests LES information for briefing, analysis, or other purposes.
- 3) **Computer storage media (e.g., CDs, disks, tapes, etc.) containing LES information will be marked “SENSITIVE” in accordance with the provisions of the ICE Information Technology (IT) Security Manual for Sensitive Systems.**
  - 4) **Portions of a classified document (i.e., subjects, titles, paragraphs, and subparagraphs) that are unclassified but contain LES information will be marked with the LES abbreviation next to the (U) designation, e.g., (U) (LES).**
  - 5) **Individual portion markings on a document that contains only LES information are not required.**

## **7. RESPONSIBILITIES.**

- 7.1** The Assistant Secretary of ICE is responsible for oversight of the policy set forth in this Directive.
- 7.2** ICE Program Office Directors are responsible for ensuring that all employees in their Program Offices comply with the provisions of this Directive.
- 7.3** ICE supervisors and managers are responsible for ensuring that their employees are aware of what constitutes FOUO and LES information and the steps necessary to safeguard such information from unauthorized disclosure. Awareness should begin upon the initial assignment of an employee and should be reinforced periodically thereafter through routine office interaction, e-mail reminders, staff meetings, or any other method or media that contributes to an informed workforce.
- 7.4** All ICE employees, detailees, and contractors are responsible for complying with the provisions of this Directive on handling and safeguarding FOUO and LES information.
- 7.5** Contractor Requirements: All offices and employees who develop requirements for contractor support are responsible for assessing the necessity of requiring application of all or part of the provisions of this Directive. When it is determined to be necessary to include some or all of these requirements in a specific ICE contract, it is the Government's responsibility to ensure that applicable portions of this Directive are identified so that they may be made a material part of the contract, thereby making contractors responsible for complying with the contract terms on handling and safeguarding FOUO and LES information. The requiring office will submit specific requirements as part of their acquisition package (along with the estimated cost for implementation).

## **8. PROCEDURES.**

- 8.1** **Control of LES Information.** ICE LES information shall be handled, stored, transmitted, and disposed of in accordance with the procedures for SBU information established in DHS MD 11042.1.
- 8.2** **Dissemination of LES Information.** ICE LES information will not be disseminated in any manner—orally, visually, or electronically—to unauthorized personnel.
- 1) Access to LES information is authorized on a "need-to-know" basis, as determined by the originator. Where there is uncertainty as to a person's need-to-know, the originator will request dissemination instructions from their next level supervisor or the originating office for the information.

- 2) Use of records and information in records that are maintained in a DHS automated information system is limited to the uses defined by the published System of Records Notice for the system.
- 3) A security clearance is not required for access to LES information; however, all persons having access to LES information must have undergone, at a minimum, a criminal history and national fingerprint check.
- 4) Information from another government agency, commonly referred to as third-party information, is subject to that agency's policy and regulations concerning discussion and dissemination of the information, unless alternative arrangements have been made.
- 5) Information designated LES may be disseminated within the Federal Government (and its contractors), and to state and local partners having a law enforcement function or a mission of public safety or protection, unless such sharing would compromise the mission of DHS or ICE or is prohibited by statute or policy.
- 6) Information designated LES may be disseminated to foreign governments and representatives having a law enforcement function or a mission of public safety or protection in compliance with ICE's authority to disclose information to foreign governments, unless such sharing would compromise the mission of DHS or ICE or is prohibited by statute or policy.
- 7) The originator must comply with any access and dissemination restrictions listed in section 8.3.
- 8) An information sharing and access agreement in the form of a memorandum of understanding (MOU) or memorandum of agreement (MOA) may formalize LES information exchanges between DHS and an external entity. MOUs and MOAs are governed by DHS MD 0450.1, entitled, "Memoranda of Understanding (MOU) and Memoranda of Agreement (MOA)," issued on January 24, 2003, and by policy documents issued by each respective ICE Program Office.
- 9) Terrorism information shall be shared with other federal agencies that have counterterrorism functions in accordance with Executive Order 13388, unless otherwise directed by the President, and consistent with any guidance issued by the Attorney General and other applicable law.

### **8.3 Limitations on Dissemination.**

- 1) ICE may disclose LES information to third parties, unless such sharing would compromise the mission of DHS or ICE or is prohibited by statute or policy.



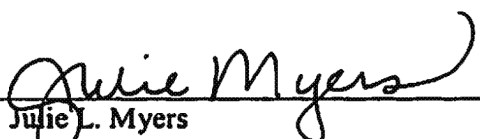
- 2) Access to the following LES information may be granted in accordance with established procedures at the discretion of the originator of the information, or the originating office only when justified by specific circumstances and a need-to-know:
  - a. Information pertaining to open investigations;
  - b. Information that reveals the identity of informants; and/or
  - c. Information pertaining to planned or ongoing surveillance and/or undercover operations and information that reveals sensitive operations.
  
- 3) ICE LES information that is protected by statute or regulation will be controlled and disseminated in accordance with the applicable guidance for that type of information. This includes, but is not limited to, the following information:
  - a. Grand Jury information – In accordance with Federal Rule of Criminal Procedure 7(e), only in the case of sharing to assist in prosecution in accordance with rule 6(e)(3)(A);
  - b. Child Victim/Witness – In accordance with 18 U.S.C. § 3509;
  - c. Juvenile – In accordance with 18 U.S.C. § 5031;
  - d. Witness Security Program – In accordance with 18 U.S.C. § 3521;
  - e. Restricted by Court Order – Dependent upon the text of the Court Order;
  - f. Proprietary – In accordance with 18 U.S.C. § 1905 or in accordance with written agreement between ICE and the provider of the information;
  - g. Federal Taxpayer Information – When information is shared with ICE by the Internal Revenue Service in accordance with 26 U.S.C. § 6103;
  - h. Critical Infrastructure Information as defined in 6 U.S.C. § 131(3) (section 212(3) of the Homeland Security Act);
  - i. Sensitive Security Information as defined in 49 C.F.R. Part 1540 and 49 U.S.C. § 40119;
  - j. Violence Against Women Claimants – In accordance with 8 U.S.C. § 1367(a)(2) (section 384(a)(2) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996);

- k. Battered Spouse or Child Information – In accordance with 8 U.S.C. § 1186a(c)(4)(c) (Immigration and Nationality Act (INA) section 216(c)(4));
  - l. Legalization/Seasonal Agricultural Worker Claims – In accordance with 8 U.S.C. § 1255a(c)(5);
  - m. Department of State Records covered by Section 222(f) of the INA – In accordance with 8 U.S.C. § 1202(f);
  - n. T Visas and U Visas – In accordance with Public Law 106-386, section 701(c)(1)(C) and pursuant to 8 C.F.R. § 214.11(e);
  - o. Temporary Protected Status – In accordance with 8 U.S.C. § 1254a(c)(6), (section 244(c)(6) of the INA);
  - p. Alien Fingerprint and Registration Forms – In accordance with 8 U.S.C. § 1304(b), section 264(b) of the INA; and
  - q. Asylum Information – In accordance with 8 C.F.R. § 208.6.
- 4) Third parties may not compel disclosure of the information to non-law enforcement organizations or persons through the use of state laws (“sunshine” laws or freedom of information laws).
- 5) Information designated as LES may not be used in legal proceedings without first consulting the originator and, in such cases, the originator should be aware that such use requires DHS approval.

9. **ATTACHMENTS.** None.

10. **NO PRIVATE RIGHT STATEMENT.** This Directive is an internal policy statement of ICE. It is not intended to and does not create any rights, privileges, or benefits, substantive or procedural, enforceable by any party against the United States; its department, agencies, or other entities; its officers or employees; or any other person.

Approved

  
 Julie L. Myers  
 Assistant Secretary  
 U.S. Immigration and Customs Enforcement