

**SAFEGUARDS:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions. The system maintains a real-time auditing function of individuals who access the system. Additional safeguards may vary by component and program.

**RETENTION AND DISPOSAL:**

ICE is in the process of drafting a proposed record retention schedule for the information maintained in IIRS, including system information stored in IFS. ICE anticipates retaining the records from other databases in IFS for 20 years, records for which IFS is the repository of record for 75 years, and ICE-generated intelligence reports for 75 years. The original electronic data containing the inputs to IFS will be destroyed after upload and verification or returned to the source.

**SYSTEM MANAGER AND ADDRESS:**

Director, ICE Office of Intelligence, 425 I Street NW., Washington DC 20536.

**NOTIFICATION PROCEDURE:**

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the component's FOIA Officer, whose contact information can be found at <http://www.dhs.gov/foia> under "contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, SW., Building 410, STOP-0550, Washington, DC 20528.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits

statements to be made under penalty or perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, <http://www.dhs.gov> or 1-866-431-0486. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you,
- Identify which component(s) of the Department you believe may have the information about you,
- Specify when you believe the records would have been created,
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records,
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) will not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

**RECORD ACCESS PROCEDURES:**

See "Notification procedure" above.

**CONTESTING RECORD PROCEDURES:**

See "Notification procedure" above.

**RECORD SOURCE CATEGORIES:**

Federal, State, local, territorial, tribal or other domestic agencies, foreign agencies, multinational or non-governmental organizations, critical infrastructure owners and operators, private sector entities and organizations, individuals, commercial data providers, and public sources such as news media outlets and the Internet.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

Pursuant to exemption 5 U.S.C. 552a(j)(2) of the Privacy Act, portions of this system are exempt from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f); and (g). Pursuant to 5 U.S.C. 552a(k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f).

Dated: December 1, 2008.

**Hugo Teufel III,**

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8-29056 Filed 12-8-08; 8:45 am]

BILLING CODE 4410-10-P

**DEPARTMENT OF HOMELAND SECURITY****Office of the Secretary**

[Docket No. DHS-2008-0132]

**Privacy Act of 1974; Immigration and Customs Enforcement (ICE)-007 Law Enforcement Support Center (LESC) Alien Criminal Response Information Management (ACRIME) System of Records**

**AGENCY:** Privacy Office, DHS.

**ACTION:** Notice of Privacy Act system of records.

**SUMMARY:** In accordance with the Privacy Act of 1974 and as part of the Department of Homeland Security's ongoing effort to review and update legacy system of records notices, the Department of Homeland Security (DHS) is giving notice that it proposes to update and reissue the following legacy record system Justice/INS. 023 Law Enforcement Support Center Database as an Immigration and Customs Enforcement (ICE) system of records titled Law Enforcement Support Center (LESC) Alien Criminal Response Information Management System (ACRIME). The information in this system of records includes data collected and maintained by the ICE LESC to carry out its mission to respond to inquiries from law enforcement agencies concerning immigration status of an individual, and whether the individual is under investigation and/or wanted by ICE or other law enforcement agencies. Categories of individuals, categories of records, and the routine uses of this legacy system of records notice have been updated. Additionally, DHS is issuing a Notice of Proposed Rulemaking (NPRM) concurrent with this SORN elsewhere in the **Federal Register**. The exemptions for the legacy system of records notices will continue to be applicable until the final rule for this SORN has been completed. This system will be included in the DHS inventory of record systems.

**DATES:** Written comments must be submitted on or before January 8, 2009. This new system will be effective January 8, 2009.

**ADDRESSES:** You may submit comments, identified by docket number DHS-2008-0132 by one of the following methods:

- *Federal e-Rulemaking Portal:* <http://www.regulations.gov>. Follow the instructions for submitting comments.
- *Fax:* 1-866-466-5370.
- *Mail:* Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of

Homeland Security, Washington, DC 20528.

- *Instructions:* All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

- *Docket:* For access to the docket to read background documents or comments received go to <http://www.regulations.gov>.

**FOR FURTHER INFORMATION CONTACT:** For general questions please contact Lyn Rahilly, Privacy Officer, (202-732-3300), Immigration and Customs Enforcement, 500 12th Street, SW., Washington, DC 20024, e-mail: [ICEPrivacy@dhs.gov](mailto:ICEPrivacy@dhs.gov). For privacy issues please contact Hugo Teufel III (703-235-0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

#### SUPPLEMENTARY INFORMATION:

##### I. Background

Pursuant to the savings clause in the Homeland Security Act of 2002, Public Law 107-296, Section 1512, 116 Stat. 2310 (November 25, 2002), the Department of Homeland Security (DHS) and its components and offices have relied on preexisting Privacy Act systems of records notices for the maintenance of records concerning the operation of the ICE Law Enforcement Support Center (LESC). The LESOC is ICE's 24-hour national enforcement operations facility. Although Title 8 U.S. Code immigration violations were the original focus of the LESOC and ACRIME under the Immigration and Naturalization Service (INS), the mission of the LESOC now supports the full range of ICE's law enforcement operations. Specifically, the LESOC provides assistance including, but not limited to, immigration status information to local, State and Federal law enforcement agencies on aliens suspected, arrested, or convicted of criminal activity, Customs violations, and violations of other laws within ICE's jurisdiction. This notice updates the preexisting system of records notice for the LESOC Database published by the legacy INS, which owned the LESOC prior to the creation of DHS. The LESOC transferred to ICE with the creation of DHS and the LESOC database is now known as the Alien Criminal Response Information Management System (ACRIME).

The ACRIME Database facilitates the response of LESOC personnel to specific inquiries from law enforcement agencies

that seek to determine the immigration status of an individual and whether the individual is under investigation and/or wanted by ICE or other law enforcement agencies. ACRIME also supports ICE's efforts to identify aliens with prior criminal convictions that may qualify them for removal from the U.S. as aggravated felons. In addition, this system of records helps to facilitate the processing of aliens for deportation or removal proceedings.

The ACRIME Database also facilitates the collection, tracking, and distribution of information about possible violations of customs and immigration law reported by the general public to the toll-free DHS/ICE Tip-line. ACRIME logs requests for assistance from criminal justice personnel who contact the LESOC on the full range of ICE law enforcement missions. ACRIME supports the entry of both administrative (immigration) and criminal arrest warrants into the Federal Bureau of Investigation's National Crime Information Center (NCIC) system. Finally, ACRIME also enables ICE to collect and analyze data to evaluate the effectiveness and quality of LESOC services and ICE's immigration law enforcement efforts.

Consistent with DHS's information sharing mission, information stored in ACRIME may be shared with other DHS components, as well as appropriate Federal, State, local, tribal, foreign, or international government agencies. This sharing will only take place after DHS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice.

In accordance with the Privacy Act of 1974 and as part of DHS's ongoing effort to review and update legacy system of records notices, DHS is giving notice that it proposes to update and reissue the following legacy record system Justice/INS. 023 Law Enforcement Support Center Database as an ICE system of records titled Law Enforcement Support Center (LESC) Alien Criminal Response Information Management System (ACRIME). The information in this system of records includes data collected and maintained both in paper form and electronically by ICE's Law Enforcement Support Center to carry out its mission to respond to inquiries from law enforcement agencies concerning immigration status of an individual, and whether the individual is under investigation and/or wanted by ICE or other law enforcement agencies. Categories of individuals, categories of

records, and the routine uses of this legacy system of records notice have been updated. Additionally, DHS is issuing a Notice of Proposed Rulemaking (NPRM) concurrent with this SORN elsewhere in the **Federal Register**. The exemptions for the legacy system of records notices will continue to be applicable until the final rule for this SORN has been completed. This system will be included in DHS's inventory of record systems.

##### II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates individuals' information. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with Privacy Act regulations, 6 CFR Part 5.

The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses of their records, and to assist individuals to more easily find such files within the agency. Below is the description of the LESOC/ACRIME system of records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this revised system of records to the Office of Management and Budget and to Congress.

#### SYSTEM OF RECORDS:

DHS/ICE-007

#### SYSTEM NAME:

Immigration and Customs Enforcement Law Enforcement Support Center Alien Criminal Response

Information Management System (LESC/ACRIME).

**SECURITY CLASSIFICATION:**

Unclassified. Law Enforcement Sensitive (LES).

**SYSTEM LOCATION:**

Records are maintained at the ICE LESC in Burlington, Vermont.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

Categories of individuals covered by this system include:

(1) Individuals covered by the Immigration and Nationality Act of 1952 (8 U.S.C. 1101 *et seq.*) and who are either the subject of an investigation, or have been arrested, charged with, and/or convicted of criminal or civil offenses that could render them removable or excludable from the U.S. under the provisions of U.S. immigration and nationality laws.

(2) Individuals who make reports to the DHS/ICE Tip-line and individuals about whom those reports were made.

(3) Individuals who are the subject of administrative (immigration) and criminal arrest warrants that the LESC has entered into the FBI's National Crime Information Center System.

(4) Individuals who are the subject of an investigation by Federal, State, local, and tribal law enforcement agencies and who have been identified through searches of shared DHS law enforcement information.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

Categories of records in this system include:

- Biographic identifiers (e.g. name, date and place of birth);
- Alien registration number ("A-number");
- Social Security Number;
- Passport number;
- Federal Bureau of Investigation (FBI) criminal history number;
- Federal, State, and local law enforcement agency booking number;
- Correctional facility inmate numbers; and

Records may also include other information, such as operator's license number, State identification number, Fingerprint Section number, and other personal identification numbers provided by law enforcement agencies, that may assist in the identification process, that would enable ICE special agents and analysts to gather additional evidence, respond to law enforcement queries, and/or to determine the status, removability, or excludability of an individual.

In addition, the system also contains information about the inquiries

submitted by Federal, State, local, and tribal law enforcement agencies and the LESC responses to those queries. Query information retained in the ACRIME database includes mandatory and optional data. Mandatory information includes: Originating Agency Identifier (ORI) number, purpose for query, attention field, phone number for requestor, name of subject of query, date of birth, sex, place of birth, custody status, and offense code. Optional information includes: alien registration number, FBI number, State system identification number, operator license number, height, weight, eye color, mother's maiden name, mother's first name, father's last name, father's first name, Social Security Number, passport number, booking number, and narrative comments entered in a remarks section.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

8 U.S.C. Sec. 1103; 8 U.S.C. Sec. 1324(b)(3); 8 U.S.C. Sec. 1360(b); 5 U.S.C. Sec. 552a(b); 5 U.S.C. Sec. 301; Section 504 of the Immigration and Nationality Act of 1990 (Pub. L. 101-649); the Federal Records Act, 44 U.S.C. 3101, Executive Order 9373..

**PURPOSE(S):**

The purpose of this system is to:

- (1) Facilitate the response of LESC personnel to specific inquiries from law enforcement agencies that seek to determine the immigration status of an individual and whether the individual is under investigation and/or wanted by ICE or other law enforcement agencies;
- (2) support ICE's efforts to identify aliens with prior criminal convictions that may qualify them for removal from the U.S. as aggravated felons;
- (3) facilitate the processing of aliens for deportation or removal proceedings;
- (4) support ICE's collection and distribution of possible violator information collected during telephone calls from the general public to DHS/ICE;
- (5) support ICE's efforts to assist Federal, State, local, and tribal criminal justice personnel who contact the LESC on the full range of ICE law enforcement missions, including both customs and immigration violations; and
- (6) enable ICE to collect and analyze data to evaluate the effectiveness and quality of LESC services and ICE's immigration law enforcement efforts.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:**

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records of information

contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (including United States Attorney Offices) or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;
2. any employee of DHS in his/her official capacity;
3. any employee of DHS in his/her individual capacity where the Department of Justice or DHS has agreed to represent the employee; or
4. the United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) or harm to the individual who relies upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To an appropriate Federal, State, local, tribal, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit and disclosure is appropriate to the proper performance of the official duties of the person making the request.

I. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or in response to a subpoena from a court of competent jurisdiction.

J. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the officer making the disclosure.

K. To Federal and foreign government intelligence or counterterrorism agencies or components where DHS becomes aware of an indication of a threat or potential threat to national or international security, or where such

use is to assist in anti-terrorism efforts and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

L. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

**DISCLOSURE TO CONSUMER REPORTING AGENCIES:**

None.

**POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:**

**STORAGE:**

Records in this system are stored electronically or on paper in secure facilities behind locked doors. Electronic records are stored on magnetic disc and digital optical media. Hardcopy records are stored in locked file cabinets.

**RETRIEVABILITY:**

Records are retrieved by name, alien registration number(s), booking number(s), FBI criminal history number(s), State criminal history number(s), Social Security Number, passport number, inmate number and other personal identifiers, and by biographic information, including place of birth, date of birth, and residential address.

**SAFEGUARDS:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

**RETENTION AND DISPOSAL:**

DHS will be working with NARA to develop the appropriate retention schedule based on the information below. The information, as collected

and maintained in ACRIME, pertains to immigration and other law enforcement investigations and national security related matters. Therefore, DHS proposes to maintain the records for seventy-five (75) years from the date of final action or case closure, after which the records will be deleted from the ACRIME system.

**SYSTEM MANAGER AND ADDRESS:**

Unit Chief, Law Enforcement Support Center, U.S. Immigration and Customs Enforcement, 188 Harvest Lane, Williston, VT 05495.

**NOTIFICATION PROCEDURE:**

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the component's FOIA Officer, whose contact information can be found at <http://www.dhs.gov/foia> under "contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, SW., Building 410, STOP-0550, Washington, DC 20528.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, <http://www.dhs.gov> or 1-866-431-0486. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you,
- Identify which component(s) of the Department you believe may have the information about you,
- Specify when you believe the records would have been created,
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records,
- If your request is seeking records pertaining to another living individual, you must include a statement from that

individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) will not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of specificity or lack of compliance with applicable regulations.

**RECORD ACCESS PROCEDURES:**

See "Notification procedure" above.

**CONTESTING RECORD PROCEDURES:**

See "Notification procedure" above.

**RECORD SOURCE CATEGORIES:**

Records are obtained from Federal, State and local law enforcement and criminal justice agencies (e.g., investigators, prosecutors, correctional institutions, police departments, and inspectors general).

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

Pursuant to exemption 5 U.S.C. 552a(j)(2) of the Privacy Act, portions of this system are exempt from subsections (c)(3) and (4); (d); (e)(1), (2), (3), (4)(G), (4)(H), (5) and (8); (f); and (g) of the Privacy Act. In addition, the system has been exempted from subsections (c)(3), (d), and (e)(1), (4)(G), (4)(H), and (f) pursuant to 5 U.S.C. 552a(k)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the **Federal Register** as additions to Title 28, Code of Federal Regulations (28 CFR 16.99). In addition, to the extent a record contains information from other exempt systems of records, ICE will rely on the exemptions claimed for those systems.

Dated: November 28, 2008.

**Hugo Teufel III,**

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8-29057 Filed 12-8-08; 8:45 am]

BILLING CODE 4410-10-P

**DEPARTMENT OF HOMELAND SECURITY**

**Office of the Secretary**

[Docket No. DHS-2008-0160]

**Privacy Act of 1974; Science & Technology Directorate-001 Research, Development, Test, and Evaluation Records System of Records**

**AGENCY:** Privacy Office, DHS.

**ACTION:** Notice of Privacy Act system of records.

**SUMMARY:** Pursuant to the Privacy Act of 1974, the Department of Homeland

Security proposes to add a new system of records titled Research, Development, Test, and Evaluation Records. This system maintains records collected in support of, or during the conduct of, Science & Technology-funded research, development, test, and evaluation activities. This new system will be added to the Department's inventory of record systems.

**DATES:** Written comments must be submitted on or before January 8, 2009. This new system will be effective January 8, 2009.

**ADDRESSES:** You may submit comments, identified by docket number DHS-2008-0160 by one of the following methods:

- *Federal e-Rulemaking Portal:* <http://www.regulations.gov>. Follow the instructions for submitting comments.

- *Fax:* 1-866-466-5370.

- *Mail:* Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

- *Instructions:* All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change and may be read at <http://www.regulations.gov>, including any personal information provided.

- *Docket:* For access to the docket to read background documents or comments received, go to <http://www.regulations.gov>.

**FOR FURTHER INFORMATION CONTACT:** For system related questions please contact the Science & Technology Directorate's Regulatory Compliance Office at [regulatorycompliance@dhs.gov](mailto:regulatorycompliance@dhs.gov). For privacy issues, please contact: Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

**SUPPLEMENTARY INFORMATION:**

**I. Background**

An integral part of the Department of Homeland Security (DHS) Science & Technology Directorate's (S&T) mission is to conduct research, development, testing, and evaluation (RDT&E activities) on topics and technologies related to improving homeland security and combating terrorism. Some RDT&E activities involve the collection of personally identifiable information. This system of records notice covers records collected in support of, or during the conduct of, DHS/S&T-funded RDT&E activities, where those records are retrieved by personal identifier.

As a general rule, the information collected will be used by DHS/S&T solely for the purposes of RDT&E activities. The information collected

will not be used for law enforcement, intelligence, or any purpose other than RDT&E. The information collected will never be used in operations and no operational decision will be based in any part on the information collected. These limitations on the use of the information collected will apply even in DHS/S&T-funded RDT&E activities in which law enforcement and/or intelligence personnel are directly involved in the activity. A different SORN, a SORN other than this SORN, is required to address any DHS/S&T-funded RDT&E activities from which information collected would be used for any purpose other than RDT&E activities.

The only exception to the above general rule limiting the use of collected information to RDT&E activities is if, during a human subject testing activity, the individual provides information that indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations. Only in that limited situation, the information collected may be referred to Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, pursuant to Routine Use G, below.

Pursuant to the Privacy Act of 1974, the Department of Homeland Security proposes to add a new system of records titled Research, Development, Test, and Evaluation Records. This system maintains records collected in support of, or during the conduct, of Science & Technology-funded research, development, test, and evaluation activities. This new system will be added to the Department's inventory of record systems.

**II. The Privacy Act**

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses and disseminates individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other particular assigned to an individual. In the Privacy Act, an individual is defined to encompass United States citizens and legal permanent residents (LPRs). As a matter of policy, DHS extends administrative Privacy Act protections