non-disclosure agreements signed.) The Administrator of the Master Roster maintains the information so as to track clearance processing and investigation information (date of investigation) and to have the most current contact information for the participants from each sector.

Dated: May 9, 2008.

Matt Coose,

Acting Chief Information Officer, National Protection and Programs Directorate, Department of Homeland Security.

[FR Doc. E8–10892 Filed 5–14–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2007–0017]

Privacy Act; Office of Intelligence and Analysis Enterprise Records System

AGENCY: Privacy Office, DHS.

ACTION: Notice of Privacy Act system of records notice.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security gives notice that it proposes to add a new system of records to its inventory of record systems, namely the Office of Intelligence & Analysis Enterprise Records System (ERS). Some of the records that were previously maintained in the Homeland Security Operations Center Database (DHS/IAIP–001), the system of records notice for which was last published in full text on April 18, 2005 (70 FR 20156), will now be part of the ERS. This notice does not rescind, revoke, or supersede the HSOC system of records notice insofar as other components of DHS maintain records within that system of records, under their respective authorities.

DATES: The new system of records will be effective June 16, 2008.

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

- *Federal eRulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments via docket number DHS–2007–0017.
- *Fax:* 1–866–466–5370.
- *Mail:* Comments by mail may also be submitted to Hugo Teufel III, Chief Privacy Officer, 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 the Information Sharing and Knowledge Management Division, Office of Intelligence and Analysis, Department of Homeland Security, Washington, DC 20528. For privacy issues, please contact: Hugo Teufel III, Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

The mission of DHS under the Homeland Security Act of 2002 is to prevent terrorist attacks; reduce the vulnerability of the United States to terrorism; minimize the damage and assist in the recovery from terrorist attacks that may occur within the United States; carry out the functions of the legacy agencies and entities transferred to the Department, including by acting as a focal point regarding natural and manmade crises and emergency planning; ensure that the functions of the agencies and subdivisions within DHS not directly related to securing the homeland are not diminished or neglected; ensure that the civil rights and civil liberties of persons within, and the overall economic security of, the United States are not diminished by efforts, activities, and programs aimed at securing the homeland; and monitor the connections between illegal drug trafficking and terrorism, coordinate efforts to sever such connections, and contribute to the effort to interdict illegal drug trafficking.

Recognizing the need for intelligence support in all of the critical mission areas identified in the President's National Strategy for Homeland Security and in direct support both of the DHS mission and all elements of the Department responsible for executing the Secretary's authorities in fulfilling it, the Under Secretary for Intelligence & Analysis, as head of the DHS Office of Intelligence and Analysis (I&A), is responsible for carrying out the responsibilities of the Secretary relating to intelligence and information analysis across the Department and, as Chief Intelligence Officer of the Department, oversees the functional integration of the Department's intelligence activities, including those occurring outside of I&A. Through successive and specific delegations issued in 2006, the Under Secretary for I&A was assigned the authority and responsibility: (1) To perform the functions specified in Title II of the Homeland Security Act that relate to the Office of Information Analysis (since renamed I&A); (2) to exercise oversight and responsibility for the functions and duties necessary to lead and manage the integration of Departmental intelligence activities; and (3) to exercise the authority under section 202 of the Homeland Security Act to ensure the timely and efficient access to all information necessary to discharge the responsibilities under section 201 of the Homeland Security Act. Taken together, the Under Secretary for I&A exercises, through I&A, lead or, in some cases, shared leadership responsibility under the Homeland Security Act for the following:

A. To access, receive, and analyze law enforcement, intelligence, and other information from federal, state, and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information, in support of the mission responsibilities of the Department and the functions of the National Counterterrorism Center established under section 119 of the National Security Act of 1947 (50 U.S.C. 404o), in order to: (A) Identify and assess the nature and scope of terrorist threats to the homeland; (B) detect and identify threats of terrorism against the United States; and (C) understand such threats in light of actual and potential vulnerabilities;

B. To request additional information from other agencies of the federal government, state and local government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary;

C. To establish Department-wide procedures for the review and analysis of information provided by State, local, and tribal governments and the private sector, integrate such information into the information gathered by the Department and other departments and agencies of the Federal Government, as appropriate, and make available such information, as appropriate, within the Department and to other departments and agencies of the Federal Government;

D. To ensure the timely and efficient access by the Secretary of Homeland Security and the Department to all information from other agencies of the federal government, including reports, assessments, analyses, and unevaluated intelligence related to threats of

terrorism against the United States and other areas under the responsibility of the Secretary, and to all information concerning infrastructure or other vulnerabilities of the United States to terrorism, necessary for assessing, analyzing, and integrating information for terrorism, homeland security, and related law enforcement and intelligence purposes under the Homeland Security Act;

E. To disseminate information analyzed by the Department within the Department, to other federal, state, and local government agencies, and to private sector entities with responsibilities relating to homeland security in order to assist in the deterrence, prevention, preemption of, or response to (including mitigation of) terrorist attacks against the United States;

F. To provide intelligence and information analysis and support to other elements of the Department;

G. To coordinate and enhance integration among the intelligence components of the Department, including through strategic oversight of the intelligence activities of such components;

H. To establish the intelligence collection, processing, analysis, and dissemination priorities, policies, processes, standards, guidelines, and procedures for the intelligence components of the Department, consistent with any directions from the President and, as applicable, the Director of National Intelligence;

I. To establish a structure and process to support the missions and goals of the intelligence components of the Department;

J. To integrate the information and standardize the format of the products of the intelligence components of the Department containing homeland security information, terrorism information, weapons of mass destruction information, or national intelligence (as defined in section 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5)));

K. To ensure that, whenever possible, the Department produces and disseminates unclassified reports and analytic products based on open-source information, and produces and disseminates such reports and analytic products contemporaneously with reports or analytic products concerning the same or similar information that the Department produced and disseminated in a classified format;

L. To ensure that intelligence information is shared, retained, and disseminated consistent with the authority of the Director of National Intelligence to protect intelligence sources and methods, and similar authorities of the Attorney General concerning sensitive law enforcement information;

M. To consult with the Director of National Intelligence and other appropriate intelligence, law enforcement, or other elements of the federal government to establish collection priorities and strategies for information, including law enforcement-related information, related to threats of terrorism against the United States through such means as the representation of the Department in discussions regarding requirements and priorities in the collection of such information;

N. To coordinate with elements of the intelligence community and with federal, state, and local law enforcement agencies and the private sector, as appropriate;

O. To assist in carrying out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks);

P. To integrate relevant information, analyses, and vulnerability assessments in order to identify priorities for protective and support measures by the Department, other federal, state, and local government agencies and authorities, the private sector, and other entities;

Q. In coordination with other agencies of the federal government, to provide specific warning information and advice about appropriate protective measures and counter-measures, to state and local government agencies and authorities, the private sector, other entities, and the public;

R. To consult with state and local governments and private sector entities to ensure appropriate exchanges of information, including law enforcement-related information, related to threats of terrorism against the United States (e.g., through information sharing networks set up under state and local fusion centers, the National Infrastructure Protection Program framework, or through the release of information to the general public through the Homeland Security Alert System);

S. To review, analyze, and make recommendations for improvements to the policies and procedures governing the sharing of information within the scope of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), including homeland security information, terrorism information, and weapons of mass destruction information, and any policies, guidelines, procedures, instructions, or standards established under that section;

T. To ensure that any material received through authorized DHS intelligence activities is protected from unauthorized disclosure and handled and used only for the performance of official duties;

U. To establish and utilize a secure communications and information technology infrastructure, including data-mining and other advanced analytic tools, to access, receive, and analyze data and information and to disseminate information acquired and analyzed by the Department, as appropriate;

V. To establish, consistent with the policies and procedures developed under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), and consistent with the enterprise architecture of the Department, a comprehensive information technology network architecture for the Office of Intelligence and Analysis that connects the various databases and related information technology assets of the Office of Intelligence and Analysis and the intelligence components of the Department in order to promote internal information sharing among the intelligence and other personnel of the Department;

W. To ensure that any information databases and analytical tools developed or utilized by the Department (A) are compatible with one another and with relevant information databases of other agencies of the federal government, and (B) treat information in such databases in a manner that complies with applicable federal law on privacy;

X. To oversee the Department's Information Sharing and Knowledge Management Officer, and those designated for each of the intelligence components of the Department, regarding coordinating the different systems used in the Department to gather and disseminate homeland security information or national intelligence (as defined in section 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5)));

Y. To coordinate training and other support to the elements and personnel of the Department, other agencies of the federal government, and state and local governments that provide information to the Department or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department;

Z. To provide to employees of the Department opportunities for training and education to develop an understanding of the definitions of homeland security information and national intelligence (as defined in section 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5))), and how information available to such employees as part of their duties might qualify as homeland security information or national intelligence, and be relevant to the Office of Intelligence and Analysis and the intelligence components of the Department;

AA. To evaluate, on an ongoing basis, how employees of the Office of Intelligence and Analysis and the intelligence components of the Department are utilizing homeland security information or national intelligence, sharing information within the Department, and participating in the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485); and

BB. To perform other duties relating to such responsibilities as the Secretary may provide.

In addition to assigning I&A the statutory responsibilities noted above, relevant provisions of the Homeland Security Act of 2002, which amended the National Security Act of 1947 in part, and subsequent amendments to Executive Order 12333, effectively designated I&A as an element of the National Intelligence Community (IC) and the position now occupied by the Under Secretary for I&A as a ''Senior Official of the Intelligence Community'' (SOIC). That, together with the Secretary's subsequent designation of the head of I&A as Chief Intelligence Officer of the Department—a dual-designation recently codified in statute through recent amendments to Title II of the Homeland Security Act of 2002—the Under Secretary for I&A now leads the integrated DHS intelligence enterprise in providing valuable, actionable intelligence and intelligence-related information for and among the National leadership, all components of DHS, the IC, and our other Federal, State, local, territorial, tribal, foreign and private sector partners.

In his December 16, 2005, memorandum concerning information sharing activities at DHS, the Secretary also assigned to what is now the position of Under Secretary for I&A the responsibility to ''develop[ ] and execut[e] the information sharing enterprise within the Department to ensure that the information and analysis provided by the Department is appropriate for providing security for the homeland * * * [and to] ensure that the sharing of intelligence and analysis between DHS and its Federal, State, local, tribal, and private sector partners is sufficient to meet their homeland security needs.''

On February 1, 2007, the Secretary formally issued the DHS Policy for Internal Information Exchange and Sharing, and in doing so, recognized that all elements of DHS are ''one agency'' for purposes of the Privacy Act and information sharing activities generally. Moreover, the Secretary specifically reaffirmed that, within the context of this ''one agency'' approach to information sharing, the acting incumbent to the position of Under Secretary for I&A is ''the official responsible for assessing and analyzing all terrorism, homeland security, and related law enforcement and intelligence information received by the Department.''

Thus, in accordance with the Privacy Act of 1974, and to facilitate the department-wide activities of I&A as described herein, the DHS gives notice that it proposes to add a new system of records to its inventory of record systems, namely the DHS I&A ERS to maintain those records associated with I&A operations, some of which existed previously in the Homeland Security Operations Center Database (HSOC) system of records. This notice does not rescind, revoke, or supersede the HSOC system of record or notice insofar as other components of DHS maintain records within this system of records, under their respective authorities.

The ERS will hold all records and information utilized by I&A to provide intelligence and analysis support to DHS, and from which I&A can cull, analyze, and fuse intelligence and related information properly received from other DHS components, and United States Government (USG) departments and agencies (including law enforcement agencies), elements of the IC, and our foreign, State, local, territorial, tribal, and private sector partners. A centrally managed records system, will allow I&A to access and communicate relevant information quickly and effectively to DHS leadership, and, as appropriate, the other entities listed above. Indeed, as defined in this notice, ERS which is a multi-domain (classified and sensitive-unclassified) national security system will enable I&A personnel to: (1) Manage intelligence requirements and leverage intelligence capabilities; (2) provide timely, actionable, and relevant intelligence information; (3) produce action-oriented indications and warnings, evaluations, and assessments of evolving terrorist capabilities and intent; (4) identify and disrupt terrorist activities against, and other threats to, our homeland and within our borders; (5) develop and employ techniques for alternative analysis; (6) facilitate the production of accurate, timely, and thorough finished intelligence products to the end-user; and (7) maintain an effective information sharing process, operations, and systems environment within and without DHS.

Given the nature of I&A's mission to ensure appropriate access to analytical information and source records while promoting a common and unified standard for data integrity, safeguarding, data exchange, and administrative oversight of the information maintained, by I&A, I&A has developed ERS as the single system of records to support all I&A operations.

The information in the ERS system of records includes intelligence information and other properly acquired information received from agencies and components of the federal government, foreign governments, organizations or entities, international organizations, state and local government agencies (including law enforcement agencies), and private sector entities, as well as information provided by individuals, regardless of the medium used to submit the information or the agency to which it was submitted. This system also contains: information regarding persons on watch lists with known or suspected links to terrorism; the results of intelligence analysis and reporting; ongoing law enforcement investigative information, information systems security analysis and reporting; active immigration, customs, border and transportation, security related records; historical law enforcement, operational, immigration, customs, border and transportation security, and other administrative records; relevant and appropriately acquired financial information; and public-source data such as that contained in media reports and commercially available databases, as appropriate. Data about the providers of information, including the means of

transmission of the data, is also retained.

I&A will use the information in the ERS system of records, consistent with its statutory responsibilities and functions listed above in sub-paragraphs A-BB of this section.

II. Legal Requirements

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the USG collects, maintains, uses and disseminates personally identifiable information.

The Privacy Act applies to information that is maintained in a system of records. A system of records is defined as a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier particular to the individual.

Individuals may request their records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR part 5.

The Privacy Act requires that each agency publish in the **Federal Register** a description denoting the type and character of each system of records to provide transparency to and notify individuals about how the USG is using personally identifiable information, to assist individuals to more easily find files within the agency, and to inform the public if any applicable Privacy Act exemptions will be claimed for the system, which would affect access to certain information contained in the system.

DHS proposes to exempt the ERS system of records from certain portions of the Privacy Act to protect classified or otherwise sensitive information that is contained in the system and to protect the integrity of ongoing counterterrorism, intelligence, law enforcement and other homeland security activities. These exemptions are necessary because ERS contains information concerning certain individuals, including but not limited to known or suspected terrorists, and activities that could impact the security of people within the United States. These exemptions are necessary, moreover, because some of the information contained in the system may be derived from sensitive intelligence, law enforcement, or other operational sources and/or acquired using sensitive intelligence or law enforcement methods.

Specifically, DHS is claiming exemptions from those provisions of the Privacy Act contained at 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f) pursuant to 5 U.S.C. 552a(k)(1), (2), (3) and (5).

Elsewhere in today's **Federal Register** is the Notice of Proposed Rulemaking for these exemptions.

Moreover, and notwithstanding those provisions of the Privacy Act from which DHS is seeking exemption today, I&A, as a member of the National Intelligence Community, also conducts its mission in conformance with the requirements of Executive Order 12333, as amended, ''United States Intelligence Activities,'' dated December 4, 1981. Section 2.3 of Executive Order 12333 requires that each agency head within the IC establish procedures to govern the collection, retention, and dissemination of information concerning U.S. Persons in a manner which protects the privacy and constitutional rights of U.S. Persons.

Specifically within I&A, intelligence personnel may acquire information which identifies a particular U.S. Person, retain it within or disseminate it from ERS, as appropriate, only when it is determined that the personally identifying information is necessary for the conduct of I&A's functions and otherwise falls into one of a limited number of authorized categories.

The routine uses covered by this system of records notice include the sharing of covered information by I&A with its homeland security partners, including, where and when appropriate, Federal, State, local, tribal, territorial, foreign, or multinational governments and agencies, and certain private sector individuals and organizations, for purposes of countering, deterring, preventing, preparing for, responding to, or recovering from natural or manmade threats, including acts of terrorism; for assisting in or facilitating the coordination of homeland security threat awareness, assessment, analysis, deterrence, prevention, preemption, and response; for assisting in authorized investigations, prosecutions or enforcement of the law, when acquired information indicates a violation or potential violation of law; where disclosure is in furtherance of I&A's information sharing responsibilities under statute or policy, including disclosure in support of those entities lawfully engaged in the collection of intelligence, counterterrorism, homeland security, and related law enforcement information; for making notifications and issuing warnings of serious threats to the homeland or to those specific individuals whose person or property may become the targets of a particular threat; and, as otherwise necessary, to properly manage and oversee the administration of this system of records and other organizational activities of I&A, including administrative responsibilities related to interagency support, litigation support, congressional affairs and oversight, records management, intelligence and information oversight, human capital, and internal security.

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

DHS/IA–001

SYSTEM NAME:

Office of Intelligence & Analysis (I&A) Enterprise Records System.

SECURITY CLASSIFICATION:

The classification of records in this system can range from UNCLASSIFIED to TOP SECRET.

SYSTEM LOCATION:

Records are maintained by the Office of Intelligence & Analysis (I&A), Department of Homeland Security, Washington, DC 20528, and at remote locations where I&A maintains secure facilities and/or conducts its mission.

CATEGORY OF INDIVIDUALS COVERED BY THE SYSTEM:

A. Individuals who are known, reasonably believed to be, or are suspected of being, involved in or linked to:

1. The existence, organization, capabilities, plans, communications, intentions, and vulnerabilities of, means of finance or material support for, and activities against or threats to the United States or United States persons and interests by, domestic, foreign or international terrorist groups and/or individuals involved in terrorism;

2. Groups or individuals believed to be assisting or associated with domestic, foreign, or international terrorist groups and/or individuals involved in terrorism;

3. Activities constituting a threat to homeland security, and/or activities that are preparatory to, or facilitate or support such activities, including:

a. Activities related to the violation or suspected violation of immigration or customs laws and regulations of the United States,

b. Activities, which could reasonably be expected to assist in the development or use of a weapon of mass effect;

c. Activities to identify, create, exploit, or undermine the vulnerabilities of the ''key resources'' (as defined in section 2(9) of the

Homeland Security Act of 2002) and ''critical infrastructure'' (as defined in 42 U.S.C. 5195c(c)) of the United States;

d. Activities to identify, create, exploit, or undermine the vulnerabilities of the cyber and national telecommunications infrastructure, including activities which may impact the availability of a viable national security and emergency preparedness communications infrastructure.

e. Activities detrimental to the security of transportation and transportation systems;

f. Activities which violate or are suspected of violating the laws relating to counterfeiting of obligations and securities of the United States and other financial crimes, including access device fraud, financial institution fraud, identity theft, computer fraud; and computer-based attacks on our nation's financial, banking, and telecommunications infrastructure;

g. Activities, not wholly conducted within the United States, which violate or are suspected of violating the laws which prohibit the production, transfer, or sale of narcotics or substances controlled in accordance with Title 21 of the United States Code, or those associated activities otherwise prohibited by Titles 21 and 46 of the United States Code;

h. Activities which impact or concern the security, safety, and integrity of our international borders, including any illegal activities that cross our borders such as violations of the immigration or customs laws of the United States;

i. Activities which impact, concern, or otherwise threaten the safety and security of the President and Vice President, their families, heads of state, and other designated individuals; the White House, Vice President's residence, foreign missions, and other designated buildings within the United States;

j. Activities which impact, concern, or otherwise threaten maritime safety and security, maritime mobility and navigation, or the integrity of the maritime environment;

k. Activities which impact, concern, or otherwise threaten the national operational capability of the Department to respond to natural and man-made major disasters and emergencies, including acts of terrorism, in support of impacted communities; to coordinate all Federal emergency management response operations, response planning and logistics programs; and to integrate Federal, State, tribal and local response programs to ensure the efficient and effective delivery of immediate emergency assistance to individuals and communities impacted by major disasters, emergencies or acts of terrorism.

l. Activities involving the detection of and response to unauthorized attempts to import, possess, store, develop, or transport nuclear or radiological material for use against the United States

4. The capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, where the individuals may be officers or employees of, or otherwise acting for or on behalf of, a foreign power or organization that may be owned or controlled, directly or indirectly, by a foreign power;

5. Intelligence activities, or other individuals known or suspected of engaging in intelligence activities, on behalf of a foreign power or terrorist group;

6. Activities or circumstances where the health or safety of that individual may be threatened, including information concerning these individuals that may be necessary for identifying and implementing protective security measures or other emergency preparedness activities;

B. Individuals who voluntarily request assistance or information, through any means, from I&A, or individuals who voluntarily provide information concerning any of the activities above, which may threaten or otherwise affect homeland security.

C. Individuals who are or have been associated with DHS or I&A activities or with the administration of the Department, including information about individuals that is otherwise required to be maintained by law or that is necessary for the provision of intelligence support to the Department.

CATEGORIES OF RECORDS IN THE SYSTEM:

I&A utilizes a single records system for maintaining I&A's operational and administrative records, including:

A. Classified and unclassified intelligence (includes national intelligence, foreign intelligence, and counterintelligence), counterterrorism, homeland security, and related law enforcement information, including source records and the reporting and results of any analysis of this information, obtained from all agencies, components and organizations of the Federal government, including the IC; foreign governments, organizations or entities, and international organizations; State, local, tribal and territorial government agencies (including law enforcement agencies); and private sector entities;

B. Information provided by record subjects and individual members of the public;

C. Information obtained from the Terrorist Screening Center, the National Counterterrorism Center, or from other organizations about individuals known or reasonably suspected of being engaged in conduct constituting, preparing for, aiding, or relating to terrorism;

D. Active and historical law enforcement investigative information;

E. Information related to lawful DHS Security investigations, including authorized physical, personnel, and communications security investigations, and information systems security analysis and reporting;

F. Operational and administrative records, including correspondence records;

G. Lawfully acquired financial information, when relevant to an authorized intelligence, counterterrorism, homeland security, or related law enforcement activity;

H. Public source data such as that contained in media, including periodicals, newspapers, broadcast transcripts, and other public reports and commercial databases; and

I. Data about the providers of any information otherwise contained within this system, including the means of transmission of the data.

Examples of information related to the ''Categories of Individuals'' listed above may include:

Full name, date of birth, gender, country of citizenship, country of birth, alien number, social security number, driver's license numbers, passport numbers, fingerprint identification number, or other unique identifying numbers, current and past home and work addresses, phone numbers, terrorist associations, biometric information including fingerprints and photographs, physical description, results from intelligence analysis related to terrorism, financial information, family members or associates, flight information, border crossing information, immigration information, or other personally identifiable information that is relevant and necessary.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; Title II and section 892 of the Homeland Security Act of 2002, Pub. L. 107–296, 116 Stat. 2145 (Nov. 25, 2002), as amended (6 U.S.C. 121, *et seq.*); 44 U.S.C. 3101; E.O. 9397; E.O. 12333; E.O. 12958; E.O. 13356; and E.O. 13388.

PURPOSE(S):

ERS replaces the applicable portions of the DHS, Homeland Security Operations Center Database (DHS/IAIP–001) system of records notice (SORN), last published in full text on April 18, 2005 [70 F.R. 20156]. The DHS/IAIP–001 SORN previously covered the functional and organizational aspects of I&A within DHS prior to realignment by the Secretary and Congress, respectively, in 2005 and 2006.

The mission-specific purposes of ERS are as follows:

A. To manage, access, analyze, integrate, and store intelligence (including national intelligence, foreign intelligence, and counterintelligence), counterterrorism, homeland security, related law enforcement, and other information to carry out the responsibilities of the Secretary of Homeland Security and the Under Secretary for I&A, as the official responsible for assessing and analyzing all terrorism, homeland security, and related law enforcement and intelligence information received by the Department, under Title II of the Homeland Security Act (6 U.S.C. 121, *et seq.*), in support of the overall DHS mission.

B. To fulfill the need for coordinated intelligence support in all of the critical mission areas specifically identified in the President's National Strategy for Homeland Security or other related activities as defined by separate Executive Order, Homeland and/or National Security Presidential Directive, or other issuance concerning the internal management and policy of Executive Branch activities.

C. To enable the provision of intelligence and analysis support to all DHS activities, components, and organizational elements, and to maintain a record system from which I&A can cull, analyze, and fuse intelligence and related information properly received from other DHS components, other United States Government (USG) departments and agencies (including law enforcement agencies), elements of the National Intelligence Community (IC), as well as our foreign, State, local, territorial, tribal, and private sector partners.

D. To permit the Under Secretary for I&A, as Chief Intelligence Officer of the Department, to foster the development and execution of an information sharing environment within DHS; to integrate the intelligence and information sharing functions and activities of the DHS intelligence enterprise to provide the most valuable, actionable intelligence and intelligence-related information for the Nation's leadership, all components of DHS, the IC, and our other partners; and to ensure both that the information and analysis provided by the Department is appropriate for providing security for the homeland and that the sharing of intelligence and analysis between DHS and its Federal, State, local, territorial, tribal, foreign, and private sector partners is sufficient to meet their respective homeland security needs.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM:

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 or 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 any Federal, State, local, tribal, territorial, foreign, or multinational government or agency, or appropriate private sector individuals and organizations, with responsibilities relating to homeland security, including responsibilities to counter, deter, prevent, prepare for, respond to, or recover from a natural or manmade threat, including an act of terrorism, or to assist in or facilitate the coordination of homeland security threat awareness, assessment, analysis, deterrence, prevention, preemption, and response;

B. To a Federal, State, local, tribal, territorial, foreign, or multinational government or agency with the responsibility and authority for investigating, prosecuting and/or enforcing a law (civil or criminal), regulation, rule, order or contract, where the record, on its face or in conjunction with other information, indicates a violation or potential violation of any such law, regulation, rule, order, or contract enforced by that government or agency;

C. To a Federal, State, local, tribal, territorial, foreign, or multinational government or agency, or other entity, including, as appropriate, certain private sector individuals and organizations, where disclosure is in furtherance of I&A's information sharing responsibilities under the Homeland Security Act of 2002, as amended, the Intelligence Reform and Terrorism Prevention Act of 2004, the National Security Act of 1947, as amended, Executive Order 12333, as amended, or any successor order, national security directive, intelligence community directive, other directive applicable to I&A, and any classified or unclassified implementing procedures promulgated pursuant to such orders and directives, or any other statute, Executive Order or directive of general applicability, and where such disclosure is otherwise compatible with the purpose for which the record was originally acquired or created by I&A;

D. To a Federal, State, local, tribal, or territorial government or agency lawfully engaged in the collection of intelligence (including national intelligence, foreign intelligence, and counterintelligence), counterterrorism, homeland security, law enforcement or law enforcement intelligence, and other information, where disclosure is undertaken for intelligence, counterterrorism, homeland security, or related law enforcement purposes, as authorized by U.S. Law or Executive Order, and in accordance with applicable disclosure policies;

E. To any other agency within the IC, as defined in section 3.4(f) of Executive Order 12333 of December 4, 1981, as amended, for the purpose of allowing that agency to determine whether the information is relevant and necessary to its mission-related responsibilities and in accordance with that agency's classified or unclassified implementing procedures promulgated pursuant to such orders promulgated pursuant to such orders and directives, or any other statute, Executive Order or directive of general applicability;

F. To foreign persons or foreign government agencies, international organizations, and multinational agencies or entities, under circumstances or for purposes mandated by, imposed by, or conferred in, Federal statute, treaty, or other international agreement or arrangement, and in accordance with applicable foreign disclosure policies, such as the National Security Decision Memorandum 119, ''Disclosure of Classified United States Military Information to Foreign Governments and International Organizations,'' which is the Presidential directive that allows for the disclosure classified information to foreign entities, and other applicable directives;

G. To any individual, organization, or entity, as appropriate, to notify them of a serious threat to homeland security for the purpose of guarding them against or responding to such a threat, or where there is a reason to believe that the recipient is or could become the target of a particular threat, to the extent the information is relevant to the protection of life, health, or property;

H. To any Federal government agency when documents or other information obtained from that agency are used in compiling the particular record, the record is also relevant to the official responsibilities of that agency, and there

otherwise exists a need for that agency to know the information in the performance of its official functions;

I. To representatives of the Department of Justice and other U.S. Government entities, to the extent necessary to obtain their advice on any matter that is within their official responsibilities to provide;

J. To the Department of Justice or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (a) DHS, or (b) any employee of DHS in his/her official capacity, or (c) any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee, or (d) the United States or any agency thereof, is a party to the litigation or has an interest in such litigation;

K. To a congressional office with information from the record of a particular individual, and in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains;

L. To individual members or staff of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, and the House Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, in connection with the exercise of the Committees' intelligence oversight and legislative functions, when such disclosures are necessary to a lawful activity of the United States, and the DHS Office of the General Counsel determines that such disclosures are otherwise lawful;

M. To the National Archives and Records Administration or other federal government agencies for the purpose of records management inspections being conducted under the authority of 44 U.S.C. sections 2904 and 2906;

N. To contractors, grantees, experts, consultants, volunteers, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government, when necessary to accomplish an agency function related to this system of records, in compliance with the Privacy Act of 1974, as amended;

O. To any agency, organization, or individual for the purposes of performing audit or oversight operations of DHS and/or I&A authorized by law, but only such information as is necessary and relevant to such audit or oversight function;

P. To the President's Foreign Intelligence Advisory Board, the Intelligence Oversight Board, any successor organizations, and any intelligence oversight entities established by the President, when the head of I&A determines that disclosure will assist these entities in the performance of their oversight functions; and

Q. To an appropriate Federal, State, local, tribal, territorial, 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 when disclosure is appropriate to the proper performance of the official duties of the person making the request.

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 in paper and/or electronic format in secure facilities. Electronic storage is on servers, CD–ROMs, DVD–ROMs, magnetic disc, tape, and digital media.

RETRIEVABILITY:

Data may be retrieved by an individual's name or other identifier, including unique identifying numbers assigned by I&A or other government agencies.

SAFEGUARDS:

Hard copy (paper) records and information in this system are maintained in a secure facility with access limited to only authorized personnel or an authorized and escorted visitor. Physical security includes security guards and locked facilities requiring badges and passwords for access.

Hard copy records are stored in vaults, safes or locked cabinets and are accessible only to authorized government personnel and contractors who are properly screened, cleared and trained in information security and the protection of privacy information.

Electronic records are maintained on and only accessible from secured systems through hardware and software devices protected by appropriate physical and technological safeguards to prevent unauthorized access, including password protection.

Electronic or digital records or information in this system are also safeguarded in accordance with applicable laws, rules, and policies, including the DHS information technology security policies and the Federal Information Security Management Act (FISMA). The protective strategies are physical, technical, administrative and environmental in nature, which provide access control to sensitive data, physical access control to DHS facilities, confidentiality of communications, authentication of sending parties, and personnel screening to ensure that all personnel with access to data are screened through background investigations commensurate with the level of access required to perform their duties.

Strict controls have been imposed to minimize the risks of compromising the information that is being stored.

Access to the computer system containing the records in this system is limited to those individuals specifically authorized and granted access under DHS regulations, who hold appropriate security clearances, and who have a need to know the information in the performance of their official duties.

Systems are also developed with an incorporated auditing function of individual use and access.

Classified information is appropriately stored in a secured certified and accredited facility, in secured databases and containers, and in accordance with other applicable requirements, including those pertaining to classified information.

Access is strictly limited to authorized personnel only.

RETENTION AND DISPOSAL:

Records in this system will be retained and disposed of in accordance with a records retention and disposal schedule to be submitted to and approved by the National Archives and Records Administration.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Information Sharing and Knowledge Management, Office of Intelligence and Analysis, Department of Homeland Security, Washington, DC 20528.

NOTIFICATION PROCEDURES:

Because this system contains classified and sensitive unclassified information related to intelligence, counterterrorism, homeland security, and law enforcement programs, records in this system have been exempted from

notification, access, and amendment to the extent permitted by subsection (k) of the Privacy Act. A request for notification of any non-exempt records in this system may be made by writing to the Disclosure Officer, Office of Intelligence and Analysis, Department of Homeland Security, Washington, DC 20528, in conformance with 6 CFR Part 5, Subpart B, which provides the rules for requesting access to Privacy Act records maintained by DHS.

RECORDS ACCESS PROCEDURES:

Because this system contains classified and sensitive unclassified information related to intelligence, counterterrorism, homeland security, and law enforcement programs, records in this system have been exempted from notification, access, and amendment to the extent permitted by subsection (k) of the Privacy Act. A request for access to non-exempt records in this system may be made by writing to the Disclosure Officer, Office of Intelligence and Analysis, Department of Homeland Security, Washington, DC 20528, in conformance with 6 CFR Part 5, Subpart B, which provides the rules for requesting access to Privacy Act records maintained by DHS.

CONTESTING RECORD PROCEDURES:

Because this system contains classified and sensitive unclassified information related to intelligence, counterterrorism, homeland security, and law enforcement programs, records in this system have been exempted from notification, access, and amendment to the extent permitted by subsection (k) of the Privacy Act. A request to amend non-exempt records in this system may be made by writing to the System Manager, identified above, in conformance with 6 CFR Part 5, Subpart B, which provides the rules for requesting access to Privacy Act records maintained by DHS.

RECORD SOURCE CATEGORIES:

Information contained in this system is obtained from individuals; other government, non-government, commercial, public, and private agencies and organizations, both domestic and foreign; media, including periodicals, newspapers, and broadcast transcripts; intelligence source documents; investigative reports, and correspondence.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

DHS has exempted this system from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f) of the Privacy Act, pursuant to 5 U.S.C. 552a(k)(1), (2), (3), and (5), as applicable. A Notice of Proposed Rulemaking for exempting this record system has been promulgated in accordance with the requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c), and (e) and is being published [in 6 CFR Part 5] concurrently with publication of this Notice Establishing a New System of Records in the **Federal Register**.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–10888 Filed 5–14–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2008–0002]

Privacy Act of 1974; System of Record

AGENCY: Privacy Office, DHS.

ACTION: Notice of Privacy system of records.

SUMMARY: Pursuant to the Privacy Act of 1974, the Department of Homeland Security, United States Coast Guard is publishing this notice of system of records entitled the Law Enforcement Information Data Base (LEIDB)/Pathfinder. A proposed rulemaking is also published in this issue of the **Federal Register** in which the Department proposes to exempt portions of this system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. Due to urgent homeland security and law enforcement mission needs, LEIDB is currently in limited operation. Recognizing that USCG is publishing a notice of system of records for an existing system, USCG will carefully consider public comments, apply appropriate revisions, and republish the LEIDB notice of system of records within 180 days of receipt of comments. Additionally, a Privacy Impact Assessment will be posted on the Department's privacy Web site. (See *http://www.dhs.gov/privacy* and follow the link to ''Privacy Impact Assessments'').

DATES: Comments must be received on or before June 16, 2008. The established system of records will be effective June 16, 2008. A revised LEIDB notice of system of records that addresses public comments and includes other USCG changes will be published not later than December 11, 2008 and will supersede this notice of system of records.

ADDRESSES: You may submit comments, identified by Docket Number DHS–2008–0002 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov*. Follow the instructions for submitting comments. All comments received will be posted without change to *http://www.regulations.gov*, including any personal information provided.
- *Fax:* 1–866–466–5370.
- *Mail:* Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

FOR FURTHER INFORMATION CONTACT: For system related questions please contact: Mr. Frank Sisto, Program Officer/System Manager LEIDB/Pathfinder, Office of ISR Systems and Technology, Data Analysis & Manipulation Division (CG–262), Phone 202–372–2795 or by mail correspondence, U.S. Coast Guard, 2100 Second Street, SW., Washington, DC 20593–0001. For privacy issues, please contact: Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background Information

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security is establishing Law Enforcement Information Data Base (LEIDB)/Pathfinder as a system to meet law enforcement information management and analysis requirements. LEIDB is currently in limited operation. LEIDB is receiving message traffic, however limitations on use of the data are in place. Coast Guard policy restricts LEIDB queries to searches that do not utilize U.S. Citizen or Lawful Permanent Resident Alien PII. Once the SORN is approved and published, new instructions will be published allowing PII searches.

LEIDB/Pathfinder was developed to efficiently manage field-created intelligence and law enforcement related reports. These intelligence reports vary in content but are submitted in a standard Coast Guard message format, which is electronically distributed through the Coast Guard Message System (CGMS) (and to a lesser extent the Defense Messaging System). CGMS is the system by which the Coast Guard manages all general message traffic to and from Coast Guard components and commands. After processing and delivering a message, CGMS archives the message for 30 days before they are deleted regardless of the content of the message.