agreement to proper use of data records contained in LEIDB/Pathfinder and must agree to meet minimum security requirements.

RETENTION AND DISPOSAL:

All records, but not including audit records maintained to document user access to information relating to specific individuals, are maintained within the system for ten (10) years. These records are then destroyed. Audit records are maintained for five years from the date of last use by any given user then destroyed.

SYSTEM MANAGER(S) AND ADDRESS:

Department of Homeland Security United States Coast Guard, Assistant Commandant for Intelligence and Criminal Investigations (CG–2), Office of ISR Systems and Technology, Data Analysis and Manipulation Division (CG–262), 2100 2nd Street, SW., Washington, DC 20593–0001.

NOTIFICATION PROCEDURE:

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 (j)(2) and (k)(1) and (k)(2) of the Privacy Act.

General inquiries regarding LEIDB/Pathfinder may be directed to Department of Homeland Security United States Coast Guard, Assistant Commandant for Intelligence and Criminal Investigations (CG–2), Office of ISR Systems and Technology, Data Analysis and Manipulation Division (CG–262), 2100 2nd Street, SW., Washington, DC 20593–0001. Submit a written request that includes your name, mailing address, social security number to the above listed system manager.

RECORD ACCESS PROCEDURE:

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 (j)(2) and (k)(1) and (k)(2) of the Privacy Act. Nonetheless, DHS will examine each separate request on a case-by-case basis, and, after conferring with the appropriate component or agency, may waive applicable exemptions in appropriate circumstances and where it would not appear to interfere with or adversely affect the law enforcement or national security purposes of the systems from which the information is recompiled or in which it is contained.

Write the FOIA/Privacy Act Officer (CG–611), FOIA/Privacy Act Request at the address given above in accordance with the ''Notification Procedure''.

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 to you 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/foia* 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.

Further information may also be found at *http://www.dhs.gov/foia.*

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 (j)(2) and (k)(1) and (k)(2) 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 LEIDB/Pathfinder is gathered from a variety of sources both internal and external to the Coast Guard. Source information may come from at sea boardings, investigations, vessel notice of arrival reports, U.S. Coast Guard personnel (both direct observations and interviews of non-Coast Guard personnel), law enforcement notices, commercial sources, as well as other federal, state, local and international agencies who are related to the maritime sector and/or national security sector.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Pursuant to 5 U.S.C. 552a(j)(2) of the Privacy Act, the records and information in this system are exempt from 5 U.S.C. 552a(c)(3) and (4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (H), and (I), (e)(5), (e)(8), (f), and (g). Pursuant to 5 U.S.C. 552a(k)(1) and (k)(2) of the Privacy Act the records and information in the system are exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f). 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 Systems of Records in the **Federal Register.**

Hugo Teufel III,

Chief Privacy Officer.

[FR Doc. E8–10894 Filed 5–14–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2008–0042]

Privacy Act of 1974; General Information Technology Access Account Records System

AGENCY: Privacy Office; DHS.

ACTION: Notice of Privacy Act system of records update.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security is giving notice that it proposes to update a system of records in its inventory. The Department of Homeland Security is updating the General Information Technology Access Account Records System system of records notice to include four new routine uses and to add to the categories of records covered by the system. The first new routine use

will allow for information sharing with federal agencies such as the Office of Personnel Management, the Merit Systems Protection Board, Office of Management and Budget, Federal Labor Relations Authority, Government Accountability Office, or the Equal Employment Opportunity Commission when information is requested in the performance of those agencies' official duties. The second routine use will allow for the routine sharing of business information outside of the Department for official purposes. This includes the sharing of business contact information to contacts outside of the Department. The third routine use allows for sharing for the purpose of investigating an alleged or proven act of identity fraud or theft. The fourth routine use allows sharing of information to regulatory and oversight bodies, including auditors, who are responsible for ensuring appropriate use of government resources.

The categories of records in the system have been updated to clarify that the information used to access DHS networks is logged and recorded, specifically user IDs, date and time of access, and the internet protocol (IP) address of the computer used to access the network. Further added to the categories of records are the names of senders and receivers of email on DHS networks.

DATES: Written comments must be submitted on or before June 16, 2008.

ADDRESSES: You may submit comments, identified by Docket Number DHS–2008–0042 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: Please identify by Docket Number Dhs–2008–0042 to request further information by one of the following methods:

- *Mail:* Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.
- *Facsimile:* 1–866–466–5370.
- *E-Mail: privacy@dhs.gov.*

SUPPLEMENTARY INFORMATION:

I. Background

As part of its efforts to streamline and consolidate its record system, the Department of Homeland Security (DHS) established the agency-wide systems of records under the Privacy Act of 1974 (5 U.S.C. 552a) called the Department of Homeland Security General Information Technology Access Account Records System (GITAARS). This system of records is part of DHS's ongoing record integration and management efforts. This system consists of information collected in order to provide authorized individuals with access to DHS information technology resources. This information includes user name, business affiliation, account information and passwords.

In order to further streamline Department operations, the GITAARS system of records notice is being updated to include four new routine uses.

The first new routine use will allow for sharing with agencies such as the Office of Personnel Management (OPM), the Merit Systems Protection Board, Federal Labor Relations Authority, the Office of Management and Budget (OMB), Government Accountability Office (GAO), and the Equal Employment Opportunity Commission in the fulfillment of these agencies' official duties. For example, agencies such as OPM conduct regular workforce surveys, which involve the need of DHS to share employee data such as an employee's name, e-mail address, gender, and race/national origin. In some cases DHS must provide, in addition or in combination to the aforementioned, other information such as: Occupation group/family, organization, supervisory status, grade, work role, duty station, series, pay plan, service in government, highest level of education, years of professional service, years of service in government, projected retirement, position title, work phone number, and work address. This new routine use allows for sharing with those agencies in furtherance of those agencies' official duties.

The second routine use added to the system of records notice allows for the routine sharing of business contact information amongst contacts, which includes but is not limited to private sector companies (contractors and non-contractors), private citizens, and other Federal, state, and local employees and agencies. This type of sharing includes the exchange of contact information through e-mail, business cards, phone conversations, and other disclosures of personal information that are routine and associated with the daily official business of the Department.

The third routine use added to the system of records notice allows for any necessary sharing of information as it relates to the investigation or resolution of an alleged or proven incident of identity theft. This sharing might include e-mail address or contact information, which may help resolve an issue of identity, among other related issues related to identity theft.

The fourth routine use added to the system of records allows for sharing with government regulatory and oversight bodies, including auditing bodies, who are responsible for ensuring appropriate use of government resources. This routine use may overlap with the first routine use noted above, but this routine use is specifically related to sharing for auditing and oversight purposes.

The categories of records have been clarified to specifically state that e-mail traffic on DHS networks is recorded (sender and recipient e-mail addresses), and that all activity on DHS networks is recorded and may be used internally at DHS or for the purposes outlined in the routine uses of this system of records notices.

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' 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 the individual or by some identifying number such as property address, or mailing address symbol, assigned to the individual. The General Information Technology Access Account Records System is such a system of records.

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 to which their records are put, and to assist individuals to more easily find such files within the agency. Below is the description of the ''General Information

Technology Access Account Records System'':

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 and to Congress.

DHS/ALL–004

SYSTEM NAME:

General Information Technology Access Account Records System, DHS/ALL–004.

SECURITY CLASSIFICATION:

Unclassified but sensitive.

SYSTEM LOCATION:

Records are maintained by the Department of Homeland Security at the DHS Data Center in Washington, DC, and at a limited number of remote locations where DHS components or programs maintain secure facilities and conducts its mission.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

A. All persons who are authorized to access DHS Information Technology resources, including employees, contractors, grantees, private enterprises and any lawfully designated representative of the above and including representatives of Federal, State, territorial, tribal, local, international, or foreign government agencies or entities, in furtherance of the DHS mission;

B. Individuals who serve on DHS boards and committees;

C. Individuals who have business with DHS and who have provided personal information in order to facilitate access to DHS Information Technology resources; and

D. Individuals who are points of contact provided for government business, operations, or programs, and the individual(s) they list as emergency contacts.

CATEGORIES OF RECORDS IN THE SYSTEM:

DHS/ALL–004 contains names, business affiliations, facility positions held, business telephone numbers, cellular phone numbers, pager numbers, numbers where individuals can be reached while on travel or otherwise away from the office, citizenship, home addresses, electronic mail addresses of senders and recipients, records on access to DHS computers and networks including user ID, date and time of access, IP address of access, logs of Internet activity, and records on the authentication of the access request; records on the names and phone numbers of other contacts, the positions or titles of those contacts, their business affiliations and other contact information provided to the Department that is derived from other sources to facilitate authorized access to DHS Information Technology resources.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; 44 U.S.C. 3101.

PURPOSE(S):

This system will collect a discrete set of personal information in order to provide authorized individuals access to or interact with DHS information technology resources. The information collected by the system will include full name, user name, account information, citizenship, business affiliation, contact information, and passwords. Directly resulting from the use of DHS information technology resources is the collection, review, and maintenance of any logs, audits, or other such security data regarding the use of such information technology resources.

The system enables DHS to maintain: (a) Account information for gaining access to information technology; (b) lists of individuals who are appropriate organizational points of contact; and (c) lists of individuals who are emergency points of contact. The system will also enable DHS to provide individuals access to certain programs and meeting attendance and where appropriate allow for sharing of information between individuals in the same operational program to facilitate collaboration.

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 or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3), limited by privacy impact assessments, data sharing, or other agreements, as follows:

A. To DHS contractors, consultants or others, when necessary to perform a function or service related to this system of records for which they have been engaged. Such recipients are required to comply with the Privacy Act of 1974, as amended (5 U.S.C. 552a).

B. To sponsors, employers, contractors, facility operators, grantees, experts, and consultants in connection with establishing an access account for an individual or maintaining appropriate points of contact and when necessary to accomplish a DHS mission function or objective related to this system of records.

C. To other individuals in the same operational program supported by an information technology system, where appropriate notice to the individual has been made that his or her contact information will be shared with other members of the same operational program in order to facilitate collaboration.

D. To a Congressional office from the record of an individual in response to an inquiry from that Congressional office made at the written or attested to request of the individual to whom the record pertains.

E. 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. Sections 2904 and 2906.

F. To the Department of Justice (DOJ), or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (a) DHS; (b) any employee of DHS in his/her official capacity; (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.

G. To federal agencies such as Office of Personnel Management, the Merit Systems Protection Board, the Office of Management and Budget, Federal Labor Relations Authority, Government Accountability Office, and the Equal Employment Opportunity Commission in the fulfillment of these agencies' official duties.

H. To international, Federal, State and local, tribal, private and/or corporate entities for the purpose of the regular exchange of business contact information in order to facilitate collaboration for official business.

I. To an appropriate Federal, State, territorial, 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.

J. To appropriate agencies, entities, and persons when: (1) It is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; (2) DHS 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) that rely upon the compromised information; and (3) the disclosure is made to such agencies, entities, and persons who are reasonably necessary to assist in DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

K. To Federal regulatory bodies, auditors, and any other oversight body charged with ensuring the appropriate use of government resources which includes but is not limited to financial, information technology, physical, and other resources.

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 on paper and/or in digital or other electronic form. Digital and other electronic images are stored on a storage area network in a secured environment. Records, whether paper or electronic, may be stored at the DHS Headquarters or at the component level. See the ''System Manager'' section below for a complete list of component system managers and contact information.

RETRIEVABILITY:

Information may be retrieved, sorted, and/or searched by an identification number assigned by computer, by facility, by business affiliation, e-mail address, or by the name of the individual, or other employee data fields previously identified in this SORN.

SAFEGUARDS:

Information in this system is safeguarded in accordance with applicable laws, rules and policies, including the DHS Information Technology Security Program Handbook. Further, GITAARS security protocols will meet multiple NIST Security Standards from Authentication to Certification and Accreditation. Records in the GITAARS will be maintained in a secure, password protected electronic system that will utilize security hardware and software to include: multiple firewalls, active intruder detection, and role-based access controls. Additional safeguards will vary by component and program. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include: restricting access to authorized personnel who have a ''need to know;'' using locks; and password protection identification features. Classified information is appropriately stored in accordance with applicable requirements. DHS file areas are locked after normal duty hours and the facilities are protected from the outside by security personnel.

RETENTION AND DISPOSAL:

Records are retained and disposed of in accordance with the National Archives and Records Administration's General Records Schedule 24, section 6, ''User Identification, Profiles, Authorizations, and Password Files.'' Inactive records will be destroyed or deleted 6 years after the user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later.

SYSTEM MANAGER(S) AND ADDRESS:

For Headquarters components of the Department of Homeland Security, the System Manager is the Director of Departmental Disclosure, U.S. Department of Homeland Security, Washington DC 20528.

For operational components that comprise the U.S. Department of Homeland Security, the System Managers are as follows:

- United States Coast Guard, FOIA Officer/PA System Manager, Commandant, CG–611, U.S. Coast Guard, 2100 2nd Street, SW., Washington, DC 20593–0001.
- United States Secret Service, FOIA/PA System Manager, Suite 3000, 950 H Street, NW., Washington, DC 20223.
- Under Secretary for Federal Emergency Management Directorate, FOIA/PA System Manager, 500 C Street, SW., Room 840, Washington, DC 20472.
- Director, Citizenship and Immigration Services, U.S. Citizenship and Immigration Services, ATTN: Records Services Branch (FOIA/PA), 111 Massachusetts Ave., NW., 2nd Floor, Washington, DC 20529.
- Commissioner, Customs and Border Protection, FOIA/PA System Manager, Disclosure Law Branch, Office of Regulations & Rulings, Ronald Reagan Building, 1300 Pennsylvania Avenue, NW. (Mint Annex), Washington, DC 20229.
- Bureau of Immigration and Customs Enforcement, FOIA/PA System Manager, Office of Investigation, Chester Arthur Building (CAB), 425 I Street, NW., Room 4038, Washington, DC 20538.
- Assistant Secretary, Transportation Security Administration, FOIA/PA System Manager, Office of Security, West Building, 4th Floor, Room 432–N, TSA–20, 601 South 12th Street, Arlington, VA 22202–4220.
- Federal Protective Service, FOIA/PA System Manager, 1800 F Street, NW., Suite 2341, Washington, DC 20405.
- Federal Law Enforcement Training Center, Disclosure Officer, 1131 Chapel Crossing Road, Building 94, Glynco, GA 31524.
- Under Secretary for Science & Technology, FOIA/PA System Manager, Washington, DC 20528.
- Under Secretary for Preparedness, Nebraska Avenue Complex, Building 81, 1st floor, Washington, DC 20528.
- Director, Operations Coordination, Nebraska Avenue Complex, Building 3, Washington, DC 20529.
- Officer of Intelligence and Analysis, Nebraska Avenue Complex, Building 19, Washington, DC 20529.

NOTIFICATION PROCEDURE:

To determine whether this system contains records relating to you, write to the appropriate System Manager(s) identified above.

RECORD ACCESS PROCEDURES:

A request for access to 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.

CONTESTING RECORD PROCEDURES:

Same as ''Records Access Procedures'' above.

RECORD SOURCE CATEGORIES:

Information contained in this system is obtained from affected individuals/organizations/facilities, public source data, other government agencies and/or information already in other DHS records systems.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–10895 Filed 5–14–08; 8:45 am]

BILLING CODE 4410–10–P