DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2008–0081]

Privacy Act of 1974: System of Records

AGENCY: Privacy Office, DHS.

ACTION: Re-publication of a Notice of Privacy system of records.

SUMMARY: Pursuant to the Privacy Act of 1974, the Department of Homeland Security is re-publishing this system of records notice (SORN) entitled the United States Coast Guard (USCG) Law Enforcement Information Data Base (LEIDB)/Pathfinder.

On May 15, 2008, DHS originally published the SORN and associated proposed rulemaking (DHS/USCG–062) in the **Federal Register**. DHS received no comments on the system of records notice and proposed rulemaking. Accordingly, DHS is republishing this SORN as final. A final rulemaking is also published in this issue of the **Federal Register** in which the Department exempts portions of this system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: The established system of records was effective as of February 29, 2008, based upon the prior LEIDB system of records notice published on January 30, 2008.

FOR FURTHER INFORMATION CONTACT: For system related questions please contact: Mike Payne (LEIDB/Pathfinder System Program Officer), Intelligence Division (CG–26), 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

Law Enforcement Information Data Base (LEIDB/Pathfinder) is operated and controlled by the United States Coast Guard, United States Department of Homeland Security. The Assistant Commandant for Intelligence and Criminal Investigations through the Office of Intelligence, Surveillance, Reconnaissance Systems and Technology, Division of Data Analysis and Manipulation (CG–262), is responsible for managing the system for the Coast Guard.

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.

The Assistant Commandant for Intelligence and Criminal Investigations (CG–2) identified a need to archive messages for more than thirty (30) days and to be able to perform analysis of the data contained within the messages to support law enforcement (LE) and intelligence activities. LEIDB/Pathfinder was developed and implemented to support these requirements.

All messages sent to the LEIDB/Pathfinder address on the CGMS are organized within LEIDB/Pathfinder based on message type (*e.g.*, Field Intelligence Report), when the information was sent, and by whom the information may be accessed. This allows for easy segregation of information based on user access controls.

Users rely on LEIDB/Pathfinder as an archival system to find and retrieve records relevant to their analyses. Users of LEIDB/Pathfinder include intelligence analysts, watch officers, field intelligence officers and intelligence staff officers, and criminal investigators. Use of LEIDB/Pathfinder obviates the need for individual analysts to compile records in a local storage system, which reduces the risk of loss or of unauthorized access to intelligence reports. Analysts rely on LEIDB/Pathfinder as the means to retrieve records. Searching through unstructured text allows the users to develop search terms that retrieve all messages relevant to an inquiry without reviewing irrelevant records. Messages contained in LEIDB/Pathfinder are not machine processed in any fashion to enable data manipulation.

LEIDB/Pathfinder includes tools for analysts to conduct data correlation, analysis, and display of data in reports. These tools enable an analyst to sort, search, and process locally stored records. LEIDB/Pathfinder does not do predictive analysis. Any search results returned to the user are based on the search criteria entered by the user. LEIDB/Pathfinder is a repository for certain CGMS messages; users must craft their own searches.

This system will contain information about physical characteristics of ports, vessels, and other maritime infrastructure. The physical characteristics may include security vulnerabilities, strengths and natural or man made attributes. This system will also contain information about individuals. The individuals will be U.S. Citizens, Lawful Permanent Residents, as well as, foreign nationals with whom the Coast Guard interacts, or can reasonably expect to interact, in the maritime environment. These individuals will be owners and operators of vessels, maritime facilities or otherwise engaged in maritime activities.

Elsewhere in today's **Federal Register**, DHS has published a final rule exempting this system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2).

Public Comments

USCG received no public comments on the original system of records notice and proposed rulemaking. Accordingly, DHS and USCG are implementing the system of records and exemptions as proposed.

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, symbol, or other identifying particular assigned to the individual.

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 recordkeeping practices transparent, to notify individuals of the uses to which personally identifiable information is put, and to assist the individual to more easily find such files within the agency.

In accordance with 5 U.S.C. 552a(r), a report concerning this record system has

been sent to the Congress and to the Office of Management and Budget.

SYSTEM OF RECORDS DHS/USCG–062

SYSTEM NAME:

Law Enforcement Information Database (LEIDB)/Pathfinder

SECURITY CLASSIFICATION:

Sensitive but unclassified to Classified, Secret.

SYSTEM LOCATION:

The computer database is located at U.S. Coast Guard Intelligence Coordination Center, Department of Homeland Security, National Maritime Intelligence Center, Washington, DC, 20395.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this notice consist of:

A. Individuals, U.S. citizens, lawful permanent residents, and foreign nationals, associated with vessels, facilities, companies, and organizations, engaged in commercial and recreational maritime activity on or adjacent to waters subject to the jurisdiction of the United States.

B. Individuals, U.S. citizens, lawful permanent residents, and foreign nationals, identified during enforcement actions taken by enforcement Officials and employees of the Coast Guard while enforcing United States (U.S.) law, international law, or treaties.

C. Individuals, U.S. citizens, resident aliens, and foreign nationals, directly and indirectly associated with individuals listed in paragraphs A and B of this section

D. Individuals, U.S. citizens, resident aliens, and foreign nationals, directly and indirectly associated with vessels, maritime facilities and other maritime infrastructure which are known, suspected, or alleged to be involved in illegal activity (e.g. contraband trafficking, illegal migrant smuggling, or terrorist activity).

E. Individuals, U.S. citizens, resident aliens, and foreign nationals, identified during a terrorist screening process as a possible identity match to a known or suspected terrorist.

F. Individuals, U.S. citizens, resident aliens, and foreign nationals, identified in or reasonably believed to be related to reports submitted by Coast Guard personnel engaged in enforcement boarding's, safety inspections, aircraft over-flights or other means of observation, and other Coast Guard operational activity.

CATEGORIES OF RECORDS IN THE SYSTEM:

LEIDB/Pathfinder contains:

A. Messages delivered to the system automatically from the Coast Guard Messaging System (CGMS) or the Defense Messaging System (DMS). Additional data records may be delivered to LEIDB/Pathfinder by Coast Guard Intelligence personnel through an electronic mail interface.

B. Field Intelligence Reports (FIR) generated by any Coast Guard unit that observes or otherwise obtains information they believe may be relevant to security threats, vulnerabilities or criminal activity.

C. Request For Information (RFI) generated by any Coast Guard unit as a request for assistance from the Intelligence program to better understand a situation.

D. Intelligence Information Report (IIR) generated by select Coast Guard units and other government agencies able to issue a standardized Department of Defense message reporting information relevant to intelligence requirements.

E. Situation Reports (SITREPS) generated by Coast Guard operational units engaged in operations providing a status update to a developing or ongoing operation.

F. Operational Status Reports (OPSTAT), generated by Coast Guard operational units to report on operational capability of personnel, units, and stations.

G. Operations Reports (OPREPS) generated by Coast Guard operational units to report the conclusion of an operation.

H. Any other operational reports in any format that contain information with intelligence value are also included and can be transmitted through CGMS or DMS.

I. Data records related to known, suspected, or alleged criminals as well as individuals associated with them (e.g. immigrants being smuggled) to include individuals engaged in terrorist activity in the Maritime domain.

J. Data records on facilities and their characteristics including: geographic location, commodities handled, equipment, certificates, inspection data, pollution incidents, casualties, and violations of all laws and international treaties, if applicable.

K. Data records on individuals associated with facilities and information pertaining to directly and indirectly related individuals, companies, and organizations associated with those facilities such as owners, operators, managers, and employees.

The above reports may have the following types of biographical information: names, aliases, dates of birth, phone numbers, addresses, nationality, identification numbers such as A-File Number, Social Security Number, or driver's license number, employer, boat registration numbers, and physical characteristics. No biometric data is collected or maintained.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Federal Records Act of 1950, Title 44 U.S.C. 3101; Title 36, Code of Federal Regulations, chapter XII; The Maritime Transportation Security Act of 2002, Pub L. 107–295 The Homeland Security Act of 2002, Pub L. 107–296; 5 U.S.C. 301; 14 U.S.C. 93, 14 U.S.C. 632; 46 U.S.C. 2306, 46 U.S.C. 3717; 46 U.S.C. 12501; 33 U.S.C. 1221 *et seq.*

PURPOSE(S):

LEIDB/Pathfinder enables Coast Guard Intelligence program personnel to manage Coast Guard message traffic that contains law enforcement information collected by Coast Guard Officers and employees in the course of their statutory duties. It also enables analysis of that information to improve the effectiveness and efficiency of Coast Guard mission performance. The Coast Guard Intelligence Program supports the full range of Coast Guard missions through data collection and analysis to meet operational Commanders information requirements. One reason for collection is to improve the awareness of operational Commanders such that they will be optimally positioned to provide services to the public. Another reason is to assist in the detection, prevention, and mitigation of all unlawful acts that occur within the maritime environment and to support responses to man made or naturally occurring threats to public safety. 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):

A. To an appropriate Federal, State, territorial, tribal, local, international, or foreign government intelligence entity, counterterrorism agency, or other appropriate authority charged with investigating threats or potential threats to national or international security or assisting in counterterrorism efforts, where a record, either on its face or in conjunction with other information, identifies a threat or potential threat to national or international security, or DHS reasonably believes the information may be useful in countering

a threat or potential treat, which includes terrorist and espionage activities, and disclosure is appropriate to the proper performance of the official duties of the person receiving the disclosure.

B. To a Federal State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

C. To appropriate Federal, state, local, tribal, foreign governmental agencies, multilateral governmental organizations, and non-governmental or private organizations for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk.

D. To U.S. Department of Defense and related entities including, but not limited to, the Military Sealift Command and the U.S. Navy, to provide safety and security information on vessels or facilities chartered, leased, or operated by those agencies.

E. To a Federal, State, or local agency responsible for response and recovery operations caused by a man made or naturally occurring disaster for use in such operations.

F. To the National Transportation Safety Board and its related State counterparts for safety investigation and transportation safety.

G. To the International Maritime Organization (IMO), intergovernmental organizations, nongovernmental organizations, or foreign governments in order to conduct investigations, operations, and inspections pursuant to its authority.

H. To Federal, State, or local agencies or foreign government agencies pertaining to marine environmental protection activities.

I. To an organization or individual in either the public or private sector, either foreign or domestic, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, to the extent the information is relevant to the protection of life or property and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

J. To contractors, grantees, experts, and consultants, performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish a DHS function related to this system of records.

K. 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.

L. 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 any component thereof, 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, 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.

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

N. 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 the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

O. To a federal, state, tribal, local or foreign government agency or organization, or international organization, lawfully engaged in collecting law enforcement intelligence information, whether civil or criminal, or charged with investigating, prosecuting, enforcing or implementing civil or criminal laws, related rules, regulations or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

No disclosure.

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

STORAGE:

Records in this system are stored in electronic form in an automated data processing (ADP) system operated and maintained by the U.S. Coast Guard. Backups are performed daily. Copies of backups are stored at an offsite location. Personal, Sensitive but Unclassified (SBU), Unclassified, and Classified data and records reside commingled with each other. Classified and non-classified information are merged on a classified domain.

Data is stored electronically. Short term data extracts may be in paper or electronic form for the duration of a specific analytic project or activity. Data extracts are stored in appropriately classified storage containers or on secured electronic media in accordance with existing security requirements.

Extracted unclassified information will be stored in accordance with DHS Management Directive governing the marking, storage, and handling of unclassified sensitive information. Unclassified information derived from LEIDB/Pathfinder remains U.S. Coast Guard information and is For Official Use Only. Determinations by any user to further disseminate, in any form, LEIDB/Pathfinder derived information to other entities or agencies, foreign or domestic, must include prior authorization from the appropriate supervisor authorized to make such determinations.

RETRIEVABILITY:

Information can be retrieved from LEIDB/Pathfinder via text string search submitted in Boolean language query format. Data records in LEIDB/Pathfinder do not rely on normalization or correlation to manipulate data, there are no prescribed data fields for LEIDB/Pathfinder data records.

Records retrieval through string searches enables data association by any term, including personal identifier. Unstructured text in a data record can be matched to any other data record. Specifically, information on individuals may be retrieved by matching individual name, Social Security Number, passport number, or the individual's relationship to a vessel (e.g., owner, shipper, consignee, crew member, passenger, etc.). Information may also be an innumerable amount of non-identifying information such as vessel name, vessel type, port location, port status, etc.

SAFEGUARDS:

Information in this system is safeguarded in accordance with applicable laws, rules and policies, including the DHS Information Technology Security Program Handbook. 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. Physical locations are locked after normal duty hours and the facilities are protected from the outside by security personnel.

LEIDB/Pathfinder falls under the security guidelines of the National Maritime Intelligence Center (NMIC) and has its own approved System Security Plan which provides that:

All classified LEIDB/Pathfinder equipment, records and storage devices are located within facilities or stored in containers approved for the storage of all levels of classified information.

All statutory and regulatory requirements pertinent to classified and unclassified information have been identified in the LEIDB/Pathfinder System Security Plan and have been implemented.

Access to records requiring SECRET level is limited strictly to personnel with SECRET or higher level clearances and who have been determined to have the appropriate ''need to know''.

Access to records requiring CONFIDENTIAL level is limited strictly to personnel with CONFIDENTIAL or higher level clearances and who have been determined to have the appropriate ''need to know''.

Access to all records is restricted by login and password protection. The scope of access to any records via login and password is further limited based on the official need of each individual authorized access. The U.S. Coast Guard will take precautions in accordance with OMB Circular A–130, Appendix III.

The U.S. Coast Guard will operate LEIDB/Pathfinder in consonance with Federal security regulations, policy, procedures, standards and guidance for implementing the Automated Information Systems Security Program. Specific Coast Guard operating rules include Command certification that an individual Officer or employee requires access to LEIDB/Pathfinder to perform official duties. Individual Officers and employees must certify knowledge of Coast Guard policies limiting the use of PII and FOUO information. Individual Officers and employees must certify 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, and 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 form 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 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 Final Rule 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 re-publication of the system of records notice, and the proposed rulemaking receiving no public comments.

Dated: September 11, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–22612 Filed 9–29–08; 8:45 am]

BILLING CODE 4410–10–P