Privacy Impact Assessment
for the

Law Enforcement Information Data Base (LEIDB)/Pathfinder

March 31, 2008

Contact Point
Mr. Frank Sisto
Coast Guard, Assistant Commandant for Intelligence and Criminal Investigations
Office of Intelligence, Surveillance, and Reconnaissance Systems and Technology, Data Analysis and Manipulation Division (CG-262)
202-372-2795

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The United States Coast Guard (USCG), a component of the Department of Homeland Security, is establishing the Law Enforcement Information Data Base (LEIDB)/Pathfinder. LEIDB/Pathfinder archives text messages prepared by individuals engaged in Coast Guard law enforcement, counter terrorism, maritime security, maritime safety and other Coast Guard missions enabling intelligence analysis of field reporting. USCG has conducted this PIA because the LEIDB/Pathfinder system collects and uses personally identifiable information (PII).

Overview

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 that is electronically distributed through the Coast Guard Message System (CGMS). 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 thirty (30) days and then CGMS deletes the messages.

The Assistant Commandant for Intelligence and Criminal Investigations (CG-2) identified a need to archive messages for more than 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 the requirement.

Messages are identified within CGMS based on the Plain Language Address (PLAD) used by an originator. LEIDB/Pathfinder has a certain PLAD address associated with it. If a USCG officer or analyst seeks to deposit a report into LEIDB/Pathfinder he adds the LEIDB/Pathfinder PLAD to the address field in CGMS. This process is much like forwarding or "cc'ing" an email recipient. Any mail traffic sent to the LEIDB/Pathfinder PLAD address will be deposited in LEIDB/Pathfinder. When this PLAD is utilized on a message that message is automatically routed by machine to the LEIDB/Pathfinder database.

All messages sent to the LEIDB/Pathfinder PLAD are organized within LEIDB/Pathfinder based on the type of message (see Question 1.1), 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, e.g., individuals with only Top Secret clearances and in the Intelligence division may access a certain set of records.

Users of the system access LEIDB/Pathfinder data via a web browser interface. The interface allows users to search for data using Boolean searches[1] that are run against the unstructured text in a message. Field Intelligence Reports (FIRs), specifically, are not required to be formatted to enable analysis; rather the requirement is to report information of potential value quickly in a free text format. Users rely on LEIDB/Pathfinder as an archival system to find and retrieve records relevant to their analysis. Use of LEIDB/Pathfinder obviates the need for individual analysts to compile records in a local storage system. Analysts rely on LEIDB/Pathfinder as the means to retrieve records. The analyst can search using developed search terms to retrieve all messages relevant to an inquiry without reviewing irrelevant records. Messages contained in LEIDB/Pathfinder are not processed in any fashion to enable data manipulation; they are not normalized so that all messages have the same data fields, or correlated so that for example if two messages have the same individual they will be automatically linked. LEIDB/Pathfinder records (see Question 1.1) 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 with whom the Coast Guard interacts with during the performance of their maritime duties. The individuals may be foreign nationals as well as U.S. citizens with whom the Coast Guard interacts with, or can reasonably expect to interact with, in the maritime environment. These individuals may be owners and operators of vessels, maritime facilities or otherwise engaged in maritime activities.

LEIDB/Pathfinder includes tools for text-based data correlation, analysis, and display of data in reports. These tools enable an analyst to sort, search, and process locally stored records. Analysts create locally stored records that are contained within data sets as defined by the system administrator and maintained in the LEIDB. LEIDB/Pathfinder contains and will process personally identifiable information (PII). LEIDB/Pathfinder does not make predictive or relationship 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 parameters.

Typical Transaction

A USCG analyst will receive an Intelligence Information Report (IIR) that is related to blue boats of a certain nationality involved in drug trafficking in the Pacific Northwest. Although the report is limited to trafficking by blue boats of a certain nationality in the Pacific Northwest, that report may be of interest to other analysts researching issues in other areas of the country. The USCG analyst will use CGMS to send the IIR to the LEIDB/Pathfinder PLAD.

To continue the example, another USCG analyst in the Key West, Florida area will, because of current issues in Key West, log onto LEIDB/Pathfinder to research blue, red, or white boats involved in drug trafficking. When researching under that set of facts, the IIR created and submitted in the Pacific Northwest may be a search result for the Key West analyst and provide the analyst with information that may be relevant to the Key West area.

Additionally, selected intelligence professionals supporting the Coast Guard Intelligence Program review CGMS for additional messages to determine if they contain information of intelligence value that was not routed to LEIDB/Pathfinder by the originator. These employees have the ability to readdress

[1] A query using the Boolean operators, AND, OR, and NOT, and parentheses to construct a complex condition from simpler criteria. A typical example is searching for combinations of keywords.

messages identified as potential valuable for intelligence purposes and deliver that message to LEIDB/Pathfinder.

LEIDB/Pathfinder is installed on the Secure Internet Protocol Router Network (SIPRNET). LEIDB/Pathfinder contains both unclassified and classified information. Message traffic originating from federal agencies and managed on the CGMS or the Defense Message Systems (DMS) are moved to the LEIDB/Pathfinder automatically and via personnel intervention with email.

Section 1.0 Characterization of the Information

1.1 What information is collected, used, disseminated, or maintained in the system?

LEIDB/Pathfinder contains an assortment of administrative and operational messages, Message type includes but is not limited to:

- 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.
- Request For Information (RFI) generated by any Coast Guard unit as a request for assistance from the Intelligence program to better understand a situation.
- 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.
- Situation Reports (SITREPS) generated by Coast Guard operational units engaged in operations providing a status update to a developing or ongoing operation.
- Operational Status Reports (OPSTAT) generated by Coast Guard operational units to report on operational capability.
- Operations Reports (OPREPS) generated by Coast Guard operational units to report the conclusion of an operation.

These messages contain information that relates to maritime activity by individuals, vessels of all types, and the maritime environment. Individuals include U.S. Citizens and Lawful Permanent Residents (LPRs) as well as foreign nationals who are lawfully present in the United States and foreign nationals who are not lawfully present in the United States. Frequently the Coast Guard conducts activities in geographic areas where all individuals encountered are foreign nationals (e.g. illegal immigrant interdictions on the high seas). The information is relevant to Coast Guard missions, including but not limited to, enforcement of laws and treaties (e.g. customs, immigration, safety and security) in and around waters subject to the jurisdiction of the United States

Messages may relate information about vessels, facilities, and other infrastructure located in the maritime environment. Messages may also contain information about cooperating sources, individuals described by cooperating sources, individuals who are subjects of enforcement activity, and individuals who are associated with the subjects of enforcement activity. Some of the data that can be expected to be collected about individuals may include by is not limited to

- name

- date of birth
- mailing address(home and work)
- telephone number (work, cell or fax)
- social security number
- email address
- employer and employment relationships
- associates – professional and personal
- passport number
- drivers license state of issuance and number
- Alien Registration Number
- Visa Number
- descriptions of individual's physical characteristics

1.2 What are the sources of the information in the system?

LEIDB/Pathfinder contains messages originating from Coast Guard Commanders. Additionally, Department of Defense organizations as well as the Central Intelligence Agency, Department of State, Department of the Treasury, and the Department of Justice send messages to the Coast Guard. All messages are delivered through the CGMS as a primary source. The Defense Message System (DMS), or other federal government message systems are also sources. Any message delivered through CGMS or DMS is deposited into LEIDB/Pathfinder through an automated process. The automated process relies on a unique address (PLAD) for LEIDB/Pathfinder that the originator must include. However, not all messages sent to the Coast Guard are automatically sent to LEIDB/Pathfinder. In some cases, authorized intelligence officers or employees may direct through a manual process other messages determined to contain information valuable to the intelligence program to the database.

USCG Commands generate messages in response to a field activity that identifies suspicious activity in the maritime environment or activity that may enhance the awareness of Coast Guard personnel responsible to provide response and prevention capability to the public. These reports may detail possible criminal or regulatory violations enforceable by the Coast Guard. Field reports include information obtained directly from private individuals, from Officers working for Federal, State, Municipal or Tribal agencies, as well as information observed by the Coast Guard personnel.

1.3 Why is the information being collected, used, disseminated, or maintained?

LEIDB/Pathfinder stores these messages to improve the effectiveness and efficiency of the Coast Guard. The Coast Guard Intelligence Program supports the full range of Coast Guard missions through data collection and analysis to meet operational Commanders information requirements. The primary reason for collection is to improve the awareness of operational Commanders so they can provide better services to the public. This information collection will aid 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.

Coast Guard's mission requires the collection of some PII about individuals found in the maritime environment. This collection enables identification of individuals who may be impacted or impact maritime security and safety or who may assist or impede the execution of Coast Guard missions.

1.4 How is the information collected?

Coast Guard personnel prepare messages to report observations, knowledge, encounters and other activities that are relevant to Coast Guard missions. These activities may include criminal enforcement encounters, safety inspections, interviews, observations, and other interactions with individuals. Information is provided in oral and written form. The results of these interactions may be reported as FIRs. This information is then transferred to a message which is collected by LEIDB/Pathfinder. LEIDB/Pathfinder does not contain any photographs or biometric data.

Messages originating from other Agencies are submitted to the Coast Guard because of the Coast Guard's missions and the Agency's determination that the message contains information that might be valuable to the Coast Guard in the performance of Coast Guard missions.

1.5 How will the information be checked for accuracy?

Accuracy of the original messages is the responsibility of the author. Data validation occurs through the analytic process and incorporation of feedback from Officers and employees of the Coast Guard operating in the field environment to which the reports pertain. All data from LEIDB/Pathfinder is compared against other data sources as part of normal analysis and data verification processes which improves the integrity of the information developed for operational Commanders.

Individual Officers and employees collecting information from individuals in the public are responsible for ensuring accurate reporting. Data records resulting from enforcement and other direct interactions with the public are reviewed by a supervisory chain prior to original dissemination. Additionally, PII contained in LEIDB/Pathfinder may be reviewed for accuracy by the individual from whom the PII is collected when not otherwise prohibited by law.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Title 14 Section 2 of the United States Code outlines the primary duties of the Coast Guard. Additionally, 14 U.S.C. §§ 81, 88, 89, 91, 94, 143, 634 and 19 U.S.C. § 1401 set out individual authorities of Coast Guard employees and the general functions and powers of the Coast Guard. Specifically, 14 U.S.C. § 93 supports this collection of information to assist the Commandant in effectively and efficiently discharging the Commandant's general powers. Individual Officers and employees act based on these authorities to obtain the information contained in LEIDB/Pathfinder. Additionally, LEIDB/Pathfinder helps create intelligence products that support Coast Guard authorities related to Ports and Waterway Safety Program (33 U.S.C. § 1221 et seq.) and Vessel Operation (46 U.S.C. § 2306).

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

LEIDB/Pathfinder centralizes a repository of information which may create the risk of proliferating access to PII beyond Officers and employees whose duties require access to the data. Technical support, system administrators, and other support personnel who require access to this information in the performance of their official duties are required to acknowledge their responsibility to protect and prevent misuse of the information.

Users are consistently reminded of this obligation. If PII is contained in a message a preformatted warning statement is added the body of the message admonishing any reader of the information to prevent unauthorized dissemination of that data record. Additionally, LEIDB/Pathfinder segregates data records to limit access to those sections of the database that a specific user may need for work performance. Users of the database are required to acknowledge the responsibility to protect the database and prevent any abuse or misuse of their access privileges.

The system itself (SIPRNET)and thus all the information on it affords a high degree of protection by requiring all authorized users to have an existing clearance that allows access to classified information. This procedure provides enhanced security to the database and security awareness to the database user which results in an overall increase in the protection afforded to the PII contained in LEIDB/Pathfinder.

Initially, USCG recognized that because LEIDB/Pathfinder is linked to the CGMS, any CGMS user could send information into LEIDB/Pathfinder simply by adding the LEIDB/Pathfinder PLAD to the address list. This means that information not intended for the purpose of analysis in LEIDB/Pathfinder would find its way into LEIDB/Pathfinder, thereby diluting the relevant messages in the database. USCG has implemented an interim policy on what information is allowed to be sent to LEIDB/Pathfinder and has begun a review of LEIDB/Pathfinder information to purge any irrelevant messages (e.g., administrative or human resources messages).

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

LEIDB/Pathfinder archives messages and enables analysis of the data records. The uses can be divided into several categories. These use categories include:

- Historical Analysis – Long term storage of selected data records.
- Matching – Comparing person or vessel name contained in messages to "look out" or watch lists.
- Link Analysis – Determining relationships, both direct and indirect, between persons identified in multiple messages.
- Trend Analysis – Identifying potential future predictions based on historical and present activity.
- Case Lead Development – Using the range of analysis to identify high potential targets that warrant focused criminal investigation.

- Baseline and Anomaly Detection – Defining levels of activity, behavior, and environmental conditions that substantiate a baseline or normal level to enable the comparison of anomaly or unique activity, behavior, and conditions that warrant further inquiry.

Other Agency Query – responding to other Agencies to assist in their missions where Coast Guard data records may be relevant.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Using the link analysis module within Pathfinder, analysts may build an association or connection between an individual to a seeming unrelated activity or person identified in a different message. However, this analysis and link is based solely on the search criteria entered by the analyst and the analysts' personal analytical skills. LEIDB/Pathfinder does not analyze data; it only returns simple search results.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The system does not use or contain commercially available data. Some publicly available data may be in the system. For instance, locally reported news stories may be incorporated by direct reference in a FIR.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The risk to privacy is that an individual user will inappropriately use the system. This risk is mitigated through training, user agreements, and ongoing audits of the system. Individual users of LEIDB/Pathfinder acknowledge, via a "user agreement" that the data contained in LEIDB/Pathfinder is sensitive and provided to the employee for use to accomplish official duties and responsibilities. LEIDB/Pathfinder is installed on the SIPRNET. All users must access SIRPNET using password protected accounts *and* a password protected LEIDB/Pathfinder account. LEIDB/Pathfinder hardware is located in a secure, classified workspace with swipe card access controls at every entry point.

Any dissemination of an LEIDB/Pathfinder data record outside of the Coast Guard must be approved at the Supervisor level within the command.

LEIDB/Pathfinder access is limited to Officers and employees within the Coast Guard Intelligence Program who have a certified need to access the system in order to provide intelligence products and situational awareness to operational Commanders and staffs responsible for planning and implementing Coast Guard operations.

Section 3.0 Retention

3.1 What information is retained?

Records contain information that relates to maritime activities by individuals, vessels of all types, and other incidents occurring in the maritime environment. Additionally, audit logs used to document user access and queries are also retained.

3.2 How long is information retained?

All records, excluding audit logs maintained to document user access and queries, are maintained for ten (10) years. These records are then destroyed. Audit logs are maintained for five (5) years, then destroyed.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

A Request for Records Disposition Authority (SF-115) has been submitted to the National Archives and Records Administration (NARA). No records will be destroyed until a NARA retention schedule is approved.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Retention of records that contain PII for ten (10) years will enable Coast Guard personnel to analyze trend and historical analysis associated with law enforcement activities. Additionally, trend and historical analysis will be utilized to identify past activities for relevant to ongoing operational requirements. It is assumed that ten (10) years will sunset the validity of most data records containing PII to any current threats. Records that may retain validity will be scrubbed of PII to facility future trend analysis that is not dependent on the PII.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Direct Access to LEIDB/Pathfinder is limited to Coast Guard Officers and employees currently performing intelligence responsibilities. Data records contained in LEIDB/Pathfinder may be shared with other intelligence and criminal enforcement entities of the Department that has a need to know the information in the performance of their official duties. Within the Department, Customs and Border

Protection (CBP), Immigration and Customs Enforcement (ICE), Citizenship and Immigration Services (CIS), United States Secret Service (USSS), Transportation Security Administration (TSA), and the Office of Intelligence and Analysis (I&A) may request and receive information derived from LEIDB/Pathfinder.

4.2 How is the information transmitted or disclosed?

Responsive data records may be shared with a requesting agency in either electronic or paper form. Electronic documents are created in a .pdf format and transferred via a secure e-mail transaction on the SIPRNET. Paper copies are either hand carried or transferred by certified/registered mail. Information can be disclosed using public or secure telephone systems.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Risks to individual privacy exist with unregulated sharing of the LEIDB/Pathfinder data records. This risk is mitigated by limiting dissemination to controlled means recognized to have inherent security features. Disclosures only occur via direct system-to-system communications where risks of third part unintended receipt is negligible.

Section 5.0 External Sharing and Disclosure

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Data records contained in LEIDB/Pathfinder may be shared with any intelligence and criminal enforcement entity of the Federal, State, Local, Tribal, international or foreign agency on a need to know basis in accordance with the routine uses identified in the applicable Privacy Act system of records notice (SORN) when the USCG believes the information will assist enforcement of civil or criminal laws.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Information relevant to the requesting agency's mission and authority can be provided to further that mission. Agencies conducting criminal investigations will be provided information on individuals who are subjects of investigation or may have information that is helpful to an investigation. Additionally, awareness information may be provided to agencies that have regulatory or response missions in the

maritime environment. The range of data records contained in LEIDB/Pathfinder may provide a source of information for State and Local officials who may not have other information sources available to determine maritime activity within there jurisdiction, each request for information will be evaluated to prevent loss or dissemination of PII that is not relevant to a requestor mission.

Any external sharing is conducted in accordance with the purpose statement and routine uses outlined in the LEIDB/Pathfinder System of Records Notice published in the Federal Register.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Responsive data records may be shared with a requesting agency in either electronic or paper form. Electronic documents are created in a .pdf form and transferred via a secure e-mail transaction on the SIPRNET when the receiving agency has that capability. Paper copies are either hand carried or transferred by certified/registered mail.

In those instances when the content of the data record is disclosed without an actual transmission of the record the disclosure is made on a secured e-mail transaction, in person, or orally using public or secure phone systems where necessary.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

The privacy risk is that data from LEIDB/Pathfinder, whether raw messages or a finished USCG intelligence product, will be shared with individuals who have no authority to see the information. Prior to disseminating any information to an external agency, USCG establishes that the recipient agency needs to know the information. Additionally, any information sharing conducted in LEIDB/Pathfinder must be done in accordance with the Privacy Act, i.e., any external sharing is conducted in accordance with the purpose statement and routine uses outlined in the LEIDB/Pathfinder System of Records Notice published in the Federal Register.

It is important to note that most information sharing conducted where LEIDB/Pathfinder data is used does not involve PII.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information?

In some instances, individuals are provided a Privacy Act notice when field Officers and employees collect information which is the basis for data records stored in LEIDB/Pathfinder. Information may be collected during an investigation of criminal or terrorism-related activities. No notice would be give as that could hamper information gathering efforts. The publication of this PIA and the publication in the Federal

Register of the System of Records Notice (SORN) and Notice of Proposed Rulemaking also serves to provide public notice of the collection, use, and maintenance of this information.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

In some cases individuals may have an opportunity or right to decline to provide information. In those instances where an Officer or employee is interviewing an individual, the individual is always free to decline to provide any information. In most cases though the LEIDB/Pathfinder contains some information that is obtained during Coast Guard enforcement operations, in which case the individual may not know that information has been collected. During these operations private individuals may be required to provide some information. The required information is maintained in a separate system (Maritime Information for Safety and Law Enforcement (MISLE)) and a Privacy Act notice is provided to those individuals.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Notice is provided through this PIA and the System of Records Notice published in the Federal Register. Individuals provide information to Officer and employees voluntarily. Those individuals who have information that is relevant to criminal investigations may be advised to cooperate directly with Special Agents. In no case are individuals informed that their identities will be protected or that the information will be limited to particular uses. All cooperating individuals are aware that the Coast Guard will use all information provided to learn more about the maritime environment and counter and respond to all threats and hazards.

Where PII is present in a message that specifically relates to intelligence or law enforcement information, individuals may not be notified that they are, for example, under investigation for criminal or terrorism-related activities. Providing such notice would hamper information gathering efforts.

Section 7.0 Access, Redress and Correction

7.1 What are the procedures that allow individuals to gain access to their information?

Individual members of the public may request copies of records from LEIDB/Pathfinder that are relevant to that individual by regular mail at the following address:

Department of Homeland Security United States Coast Guard, FOIA/Privacy Act Officer (CG-611), FOIA/Privacy Act Request, 2100 2nd Street, SW, Washington, DC 20593-0001.

Each request will be evaluated and all records will be provided to the requestor to the extent permitted by law.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Individuals may request record correction by citing the error contained in a record and by providing the corrected information. The request must include a rational basis for the correction as well as a source, which could be a person, document, or other evidence, for the correction. All correspondence is address 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

7.3 How are individuals notified of the procedures for correcting their information?

Procedures for correcting the data are contained in the SORN. The SORN states: "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 (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."

7.4 If no formal redress is provided, what alternatives are available to the individual?

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 (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.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

These rights are provided to the extent practicable for USCG operations. Despite being exempted under the Privacy Act, USCG will respond to any information requests on a case by case basis where compliance would not hinder or unduly burden USCG operations. Privacy risks associated with redress include the collection of additional information on the individuals. Risks are mitigated by handling the information in the same way other data is handled.

Section 8.0 Technical Access and Security

8.1 What procedures are in place to determine which users may access the system and are they documented?

LEIDB/Pathfinder user groups include system administrators, data managers, intelligence analysts, and law enforcement personnel. User groups include contractors and Coast Guard personnel. Users are also grouped according to the command which they are assigned for greater control. Users from each group are assigned to a user role.

User roles in LEIDB/Pathfinder include Administrators (system administrators and data managers), LE (law enforcement), and IC (intelligence). Administrators have complete access to data and capabilities and are responsible for creating accounts and administering roles. LE users have access to FIRs, IC users have access to all database files.

8.2 Will Department contractors have access to the system?

Yes, as defined in section 8.1, to the extent the terms of the contract require the contractor to have access to support the purposes of the contract.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Coast Guard provides FOIA/Privacy Act training as required by the FOIA/Privacy Act manual (COMDTINST M5260.3) to all Coast Guard employees and contractors. Additionally, occasional reminders such as All Coast Guard message 427/07 Subj: Safeguarding Personal Privacy Information highlights the sensitive nature of PII and requires refresher training on applicable policy.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes. As a system certified and accredited for operation on the SIPRNET, the Coast Guard relies on the System Security Authorization Agreement (SSAA) and Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP).

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Several safeguards are implemented in LEIDB/Pathfinder. These include segregation of data, individual and unique user names and system audit logs. Every user accessing LEIDB/Pathfinder has unique user identification. Using various tools included in the LEIDB/Pathfinder, the data manager can query system generated audit logs to determine what queries were executed by any user and if the user was an authorized user. The system manager is required to conduct a user audit at least every six months, actual frequency of audit may increase as system use changes, but semi-annual audits will remain a minimum standard.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Data access is controlled and limited to those individuals who need to manage the system or use the system to further Coast Guard mission performance. Law enforcement duties and analysis that supports law enforcement require awareness and sensitivity to privacy issues and concerns. Loss of data and proliferation of data were identified as concerns which are mitigated by limiting operation of the system to the SIPRNET, introducing inherent access limitations, and limiting user groups to those with assigned duties that are certified to require access.

Section 9.0 Technology

9.1 What type of project is the program or system?

LEIDB/Pathfinder is an operational system that provides analytical support tools to Coast Guard maritime analysts.

9.2 What stage of development is the system in and what project development lifecycle was used?

The Pathfinder system was developed by and is provided system support from the National Ground Intelligence Center (NGIC). The NGIC provides core system upgrades and patches. The LEIDB/Pathfinder

implementation installed at the NMIC is supported by personnel assigned to CG-2. There is no development work being done on LEIDB/Pathfinder, only routine operational maintenance.

All data dictionaries, data models, system architecture and process flows are maintained and managed by NGIC personnel.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

The LEIDB/Pathfinder system employs analysis technologies that enable an analysis to build relationships between records that may not have direct relationships. Relationships realized by this initial analysis will be further scrutinized by analysis and verified using other data sources. Previously, this information could not be easily analyzed for possible relationships. The system could incorrectly identify relationships, which would impact privacy; however, the system is set up so that a trained analyst reviews the relationships and is able to break the relationship, if it is incorrect. Through both technology and training, the system has mitigated the privacy risks associated with the system.

Approval Signature Page

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security