

subjects of counterterrorism or law enforcement investigations to the fact of those investigations then not previously known.

(10) From subsection (e)(12) (Matching Agreements) because requiring DHS to provide notice of alterations to existing matching agreements would impair DHS operations by indicating which data elements and information are valuable to DHS's analytical functions, thereby providing harmful disclosure of information to individuals who would seek to circumvent or interfere with DHS's missions.

(11) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

**Hugo Teufel III,**

*Chief Privacy Officer, Department of Homeland Security.*

[FR Doc. E8-22606 Filed 9-29-08; 8:45 am]

**BILLING CODE 4410-10-P**

## DEPARTMENT OF HOMELAND SECURITY

### Office of the Secretary

#### 6 CFR Part 5

[Docket No. DHS-2008-0082]

### Privacy Act of 1974: Implementation of Exemptions; U.S. Coast Guard Law Enforcement Information Database (LEIDB)/Pathfinder

**AGENCY:** Privacy Office, DHS.

**ACTION:** Final rule.

**SUMMARY:** On May 15, 2008, the Department of Homeland Security originally published the SORN and associated proposed rulemaking for the United States Coast Guard Law Enforcement Information Data Base (LEIDB/Pathfinder) (DHS/USCG-062) in the **Federal Register**. The Department of Homeland Security is issuing a final rule to amend its regulations to exempt portions of an existing system of records entitled the USCG LEIDB/Pathfinder from certain provisions of the Privacy Act. Specifically, the Department exempts portions of the LEIDB/Pathfinder system from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

**DATES:** *Effective Date:* This final rule is effective September 30, 2008.

**FOR FURTHER INFORMATION CONTACT:**

Department of Homeland Security United States Coast Guard, Mike Payne (LEIDB/Pathfinder System Program Officer), Intelligence Division (CG-26), 2100 2nd Street, SW., Washington, DC 20593-0001; Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of Homeland Security,

Washington, DC 20528; telephone 703-235-0780.

**SUPPLEMENTARY INFORMATION:**

#### Background

The Department of Homeland Security (DHS) published a notice of proposed rulemaking in the **Federal Register**, 73 FR 28060, 15 May 2008, proposing to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. The system of records is the United States Coast Guard (USCG) Law Enforcement Intelligence Data Base (LEIDB/Pathfinder). The LEIDB system of records notice (SORN) was published concurrently in the **Federal Register**, 73 FR 28135, May 15, 2008, and comments were invited on both the proposed rule and SORN. No comments were received. Accordingly, the Department is adopting the proposed rule as final. Concurrently in this issue of the **Federal Register**, DHS is re-publishing the SORN for USCG LEIDB/Pathfinder.

This Final Rule is also updating the justification for exempting LEIDB/Pathfinder from section (e)(5) of the Privacy Act. The prior justification referenced the receipt of information from "foreign agency record systems." LEIDB/Pathfinder does not receive information directly from any foreign source. Any information received from a foreign source would be evaluated and input into a USCG message as written by a USCG officer or crewman. The USCG drafted message may ultimately arrive in LEIDB. The justification has been narrowed to more accurately reflect this fact (see justifications below at Part 5, sub 6(b)(8)).

Lastly, a Privacy Impact Assessment for LEIDB/Pathfinder is posted on the Department's privacy Web site. (See <http://www.dhs.gov/privacy> and follow the link to "Privacy Impact Assessments").

Pursuant to the requirements of the Regulatory Flexibility Act, 5 U.S.C. 601-612, DHS certifies that these regulations will not significantly affect a substantial number of small entities. The final rule imposes no duties or obligations on small entities. Further, in accordance with the provisions of the Paperwork Reduction Act of 1995, 44 U.S.C. 3501, DHS has determined that this final rule would not impose new record keeping, application, reporting, or other types of information collection requirements.

#### Public Comments

USCG received no comments on the system of records notice or notice of proposed rulemaking. Accordingly, DHS

and USCG will implement the rulemaking as proposed.

#### Regulatory Requirements

##### A. Regulatory Impact Analyses

Changes to Federal regulations must undergo several analyses. In conducting these analyses, DHS has determined:

##### 1. Executive Order 12866 Assessment

This rule is not a significant regulatory action under Executive Order 12866, "Regulatory Planning and Review" (as amended). Accordingly, this rule has not been reviewed by the Office of Management and Budget (OMB). Nevertheless, DHS has reviewed this rulemaking and concluded that there will not be any significant economic impact.

##### 2. Regulatory Flexibility Act Assessment

Pursuant to section 605 of the Regulatory Flexibility Act (RFA), 5 U.S.C. 605(b), as amended by the Small Business Regulatory Enforcement and Fairness Act of 1996 (SBREFA), DHS certifies that this rule will not have a significant impact on a substantial number of small entities. The rule would impose no duties or obligations on small entities. Further, the exemptions to the Privacy Act apply to individuals, and individuals are not covered entities under the RFA.

##### 3. International Trade Impact Assessment

This rulemaking will not constitute a barrier to international trade. The exemptions relate to criminal investigations and agency documentation and, therefore, do not create any new costs or barriers to trade.

##### 4. Unfunded Mandates Assessment

Title II of the Unfunded Mandates Reform Act of 1995 (UMRA), (Pub. L. 104-4, 109 Stat. 48), requires Federal agencies to assess the effects of certain regulatory actions on State, local, and tribal governments, and the private sector. This rulemaking will not impose an unfunded mandate on State, local, or tribal governments, or on the private sector.

##### B. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501 *et seq.*) requires that DHS consider the impact of paperwork and other information collection burdens imposed on the public and, under the provisions of PRA section 3507(d), obtain approval from the Office of Management and Budget (OMB) for each collection of information it conducts, sponsors, or requires through regulations. DHS has

determined that there are no current or new information collection requirements associated with this rule.

### C. Executive Order 13132, Federalism

This action will not have a substantial direct effect on the States, on the relationship between the national Government and the States, or on the distribution of power and responsibilities among the various levels of government, and therefore will not have federalism implications.

### D. Environmental Analysis

DHS has reviewed this action for purposes of the National Environmental Policy Act of 1969 (NEPA) (42 U.S.C. 4321–4347) and has determined that this action will not have a significant effect on the human environment.

### E. Energy Impact

The energy impact of this action has been assessed in accordance with the Energy Policy and Conservation Act (EPCA) Public Law 94–163, as amended (42 U.S.C. 6362). This rulemaking is not a major regulatory action under the provisions of the EPCA.

### List of Subjects in 6 CFR Part 5

Freedom of information; Privacy.

■ For the reasons stated in the preamble, DHS amends Chapter I of Title 6, Code of Federal Regulations, as follows:

## PART 5—DISCLOSURE OF RECORDS AND INFORMATION

■ 1. The authority citation for Part 5 continues to read as follows:

**Authority:** Pub. L. 107–296, 116 Stat. 2135, 6 U.S.C. 101 *et seq.*; 5 U.S.C. 301. Subpart A also issued under 5 U.S.C. 552.

■ 2. At the end of Appendix C to Part 5, add the following new paragraph 9 to read as follows:

### Appendix C to Part 5—DHS Systems of Records Exempt From the Privacy Act

\* \* \* \* \*

9. The Law Enforcement Information Data Base (LEIDB)/Pathfinder is a historical repository of selected Coast Guard message traffic. LEIDB/Pathfinder supports law enforcement intelligence activities. LEIDB/Pathfinder users can query archived message traffic and link relevant information across multiple data records within LEIDB/Pathfinder. Users have system tools enabling the user to identify potential relationships between information contained in otherwise unrelated documents. These tools allow the analysts to build high precision and low return queries, which minimize false hits and maximize analyst productivity while working with unstructured, unformatted, free text documents.

(a) Pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2) certain records or information in

the above mentioned system of records are exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (e)(5), and (8); (f), and (g). These exemptions apply only to the extent that information in this system is subject to exemption. Where compliance would not appear to interfere with or adversely affect the intelligence, counterterrorism, homeland security, and related law enforcement purposes of this system, the applicable exemption may be waived by DHS.

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) (Accounting for Disclosures) because making available to a record subject the accounting of disclosures from records concerning him/her would specifically reveal any interest in the individual of an intelligence, counterterrorism, homeland security, or related investigative nature. Revealing this information could reasonably be expected to compromise ongoing efforts of the Department to identify, understand, analyze, investigate, and counter the activities of:

(i) Known or suspected terrorists and terrorist groups;

(ii) Groups or individuals known or believed to be assisting or associated with known or suspected terrorists or terrorist groups;

(iii) Individuals known, believed to be, or suspected of being engaged in activities constituting a threat to homeland security, including (1) activities which impact or concern the security, safety, and integrity of our international borders, including any illegal activities that either cross our borders or are otherwise in violation of the immigration or customs laws and regulations of the United States; (2) activities which could reasonably be expected to assist in the development or use of a weapon of mass effect; (3) activities meant to identify, create, or exploit the vulnerabilities of, or undermine, the “key resources” (as defined in section 2(9) of the Homeland Security Act of 2002) and “critical infrastructure” (as defined in 42 U.S.C. 5195c(c)) of the United States, including the cyber and national telecommunications infrastructure and the availability of a viable national security and emergency preparedness communications infrastructure; (4) activities detrimental to the security of transportation and transportation systems; (5) activities which violate or are suspected of violating the laws relating to counterfeiting of obligations and securities of the United States and other financial crimes, including access device fraud, financial institution fraud, identity theft, computer fraud; and computer-based attacks on our nation’s financial, banking, and telecommunications infrastructure; (6) activities, not wholly conducted within the United States, which violate or are suspected of violating the laws which prohibit the production, transfer, or sale of narcotics or substances controlled in accordance with Title 21 of the United States Code, or those associated activities otherwise prohibited by Titles 21 and 46 of the United States Code; (7) activities which impact, concern, or otherwise threaten the safety and security of

the President and Vice President, their families, heads of state, and other designated individuals; the White House, Vice President’s residence, foreign missions, and other designated buildings within the United States; (8) activities which impact, concern, or otherwise threaten domestic maritime safety and security, maritime mobility and navigation, or the integrity of the domestic maritime environment; (9) activities which impact, concern, or otherwise threaten the national operational capability of the Department to respond to natural and manmade major disasters and emergencies, including acts of terrorism; (10) activities involving the importation, possession, storage, development, or transportation of nuclear or radiological material without authorization or for use against the United States;

(iv) Foreign governments, organizations, or persons (foreign powers); and

(v) Individuals engaging in intelligence activities on behalf of a foreign power or terrorist group.

Thus, by notifying the record subject that he/she is the focus of such efforts or interest on the part of DHS, or other agencies with whom DHS is cooperating and to whom the disclosures were made, this information could permit the record subject to take measures to impede or evade such efforts, including the taking of steps to deceive DHS personnel and deny them the ability to adequately assess relevant information and activities, and could inappropriately disclose to the record subject the sensitive methods and/or confidential sources used to acquire the relevant information against him/her. Moreover, where the record subject is the actual target of a law enforcement investigation, this information could permit him/her to take measures to impede the investigation, for example, by destroying evidence, intimidating potential witnesses, or avoiding detection or apprehension.

(2) From subsection (c)(4) (Accounting for Disclosure, notice of dispute) because certain records in this system are exempt from the access and amendment provisions of subsection (d), this requirement to inform any person or other agency about any correction or notation of dispute that the agency made with regard to those records, should not apply.

(3) From subsections (d)(1), (2), (3), and (4) (Access to Records) because these provisions concern individual rights of access to and amendment of records (including the review of agency denials of either) contained in this system, which consists of intelligence, counterterrorism, homeland security, and related investigatory records concerning efforts of the Department, as described more fully in subsection (b)(1), above. Compliance with these provisions could inform or alert the subject of an intelligence, counterterrorism, homeland security, or investigatory effort undertaken on behalf of the Department, or by another agency with whom DHS is cooperating, of the fact and nature of such efforts, and/or the relevant intelligence, counterterrorism, homeland security, or investigatory interest of DHS and/or other intelligence, counterterrorism, or law enforcement agencies. Moreover,

compliance could also compromise sensitive information either classified in the interest of national security, or which otherwise requires, as appropriate, safeguarding and protection from unauthorized disclosure; identify a confidential source or disclose information which would constitute an unwarranted invasion of another individual's personal privacy; reveal a sensitive intelligence or investigative technique or method, including interfering with intelligence or law enforcement investigative processes by permitting the destruction of evidence, improper influencing or intimidation of witnesses, fabrication of statements or testimony, and flight from detection or apprehension; or constitute a potential danger to the health or safety of intelligence, counterterrorism, homeland security, and law enforcement personnel, confidential sources and informants, and potential witnesses. Amendment of the records would interfere with ongoing intelligence, counterterrorism, homeland security, and law enforcement investigations and activities, including incident reporting and analysis activities, and impose an impossible administrative burden by requiring investigations, reports, and analyses to be continuously reinvestigated and revised.

(4) From subsection (e)(1) (Relevant and Necessary) because it is not always possible for DHS to know in advance of its receipt the relevance and necessity of each piece of information it acquires in the course of an intelligence, counterterrorism, or investigatory effort undertaken on behalf of the Department, or by another agency with whom DHS is cooperating. In the context of the authorized intelligence, counterterrorism, and investigatory activities undertaken by DHS personnel, relevance and necessity are questions of analytic judgment and timing, such that what may appear relevant and necessary when acquired ultimately may be deemed unnecessary upon further analysis and evaluation. Similarly, in some situations, it is only after acquired information is collated, analyzed, and evaluated in light of other available evidence and information that its relevance and necessity can be established or made clear. Constraining the initial acquisition of information included within the LEIDB in accordance with the relevant and necessary requirement of subsection (e)(1) could discourage the appropriate receipt of and access to information which DHS and USCG are otherwise authorized to receive and possess under law, and thereby impede efforts to detect, deter, prevent, disrupt, or apprehend terrorists or terrorist groups, and/or respond to terrorist or other activities which threaten homeland security. Notwithstanding this claimed exemption, which would permit the acquisition and temporary maintenance of records whose relevance to the purpose of the LEIDB may be less than fully clear, DHS will only disclose such records after determining whether such disclosures are themselves consistent with the published LEIDB routine

uses. Moreover, it should be noted that, as concerns the receipt by USCG, for intelligence purposes, of information in any record which identifies a U.S. Person, as defined in Executive Order 12333, as amended, such receipt, and any subsequent use or dissemination of that identifying information, is undertaken consistent with the procedures established and adhered to by USCG pursuant to that Executive Order. Specifically, USCG intelligence personnel may acquire information which identifies a particular U.S. Person, retain it within or disseminate it from LEIDB, as appropriate, only when it is determined that the personally identifying information is necessary for the conduct of USCG's functions, and otherwise falls into one of a limited number of authorized categories, each of which reflects discrete activities for which information on individuals would be utilized by the Department in the overall execution of its statutory mission.

(5) From subsection (e)(2) (Collection of Information from Individuals) because application of this provision could present a serious impediment to counterterrorism or law enforcement efforts in that it would put the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct designed to frustrate or impede that activity. The nature of counterterrorism, and law enforcement investigations is such that vital information about an individual frequently can be obtained only from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely solely upon information furnished by the individual concerning his own activities.

(6) From subsection (e)(3) (Notice to Subjects), to the extent that this subsection is interpreted to require DHS to provide notice to an individual if DHS or another agency receives or collects information about that individual during an investigation or from a third party. Should the subsection be so interpreted, exemption from this provision is necessary to avoid impeding counterterrorism or law enforcement efforts by putting the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct intended to frustrate or impede that activity.

(7) From subsections (e)(4) (G), (H) and (I) (Access), inasmuch as it is unnecessary for the publication of rules and procedures contemplated therein since the LEIDB, pursuant to subsections (2) and (3), above, will be exempt from the underlying duties to provide to individuals notification about, access to, and the ability to amend or correct the information pertaining to them in, this system of records. Furthermore, to the extent that subsection (e)(4)(I) is construed to require more detailed disclosure than the information accompanying the system notice for LEIDB, as published in today's **Federal Register**, exemption from it is also necessary to protect the confidentiality, privacy, and

physical safety of sources of information, as well as the methods for acquiring it. Finally, greater specificity concerning the description of categories of sources of properly classified records could also compromise or otherwise cause damage to the national or homeland security.

(8) From subsection (e)(5) (Collection of Information) because many of the records contained in this system are derived from other domestic and foreign sources, it is not possible for DHS to vouch for those records' compliance with this provision; however, the DHS has implemented internal quality assurance procedures to ensure that data used in its screening processes is as complete, accurate, and current as possible. In addition, in the collection of information for law enforcement and counterterrorism purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by (e)(5) would limit the ability of those agencies' trained investigators and intelligence analysts to exercise their judgment in conducting investigations and impede the development of intelligence necessary for effective law enforcement and counterterrorism efforts.

(9) From subsection (e)(8) (Notice on Individuals) because to require individual notice of disclosure of information due to compulsory legal process would pose an impossible administrative burden on DHS and other agencies and could alert the subjects of counterterrorism or law enforcement investigations to the fact of those investigations then not previously known.

(10) From subsection (f) (Agency Rules) because portions of this system are exempt from the access and amendment provisions of subsection (d). Access to, and amendment of, system records that are not exempt or for which exemption is waived may be obtained under procedures described in the related SORN or Subpart B of this Part.

(11) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

**Hugo Teufel III,**

*Chief Privacy Officer, Department of Homeland Security.*

[FR Doc. E8-22613 Filed 9-29-08; 8:45 am]

**BILLING CODE 4410-10-P**