Proposed Rules

Federal Register
Vol. 73, No. 95
Thursday, May 15, 2008

This section of the FEDERAL REGISTER contains notices to the public of the proposed issuance of rules and regulations. The purpose of these notices is to give interested persons an opportunity to participate in the rule making prior to the adoption of the final rules.

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary; Privacy Office

6 CFR Part 5

[Docket No. DHS–2007–0018]

Privacy Act of 1974: Implementation of Exemptions: The Office of Intelligence and Analysis Enterprise Records System

AGENCY: Privacy Office, DHS.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security is concurrently establishing a new system of records pursuant to the Privacy Act of 1974 [5 U.S.C. 552a], as amended, to cover records maintained by the Office of Intelligence and Analysis. These records were previously covered by the Department of Homeland Security, Homeland Security Operations Center Database [DHS/IAIP–001], last published in full text on April 18, 2005 [70 FR 20156]. In this proposed rulemaking, the Department of Homeland Security proposes to exempt this new system of records, entitled the Office of Intelligence and Analysis Enterprise Records System (ERS) [DHS/IA–001], from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k). As explained in the proposed rule, the exemption is necessary to avoid interference with the intelligence, counterterrorism, and other homeland security responsibilities, and any related law enforcement functions of the Department of Homeland Security and its Office of Intelligence and Analysis. Public comment is invited.

DATES: Comments must be received on or before June 16, 2008.

ADDRESSES: You may submit comments, identified by DOCKET NUMBER DHS–2007–0023 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments via docket number DHS–2007–0018.
- *Fax:* 1–866–466–5370.
- *Mail:* Hugo Teufel III, DHS Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528.
- *Instructions:* All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.
- *Docket:* For access to the docket to read background documents or comments received go to *http://www.regulations.gov.*
- *Hand Delivery/Courier:* Hugo Teufel III, Chief Privacy Officer, Department of Homeland Security, 245 Murray Lane, SW., Building 410, Washington, DC 20528, 7:30 a.m. to 4 p.m.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact the Director, Information Sharing and Knowledge Management Division, Office of Intelligence and Analysis, Department of Homeland Security, Washington, DC 20528, at (202) 282–8248. For privacy issues, please contact: Hugo Teufel III (571–227–3813), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528, E-mail: *PIA@dhs.gov.*

SUPPLEMENTARY INFORMATION:

Background

Elsewhere in today's **Federal Register**, the Department of Homeland Security (DHS) is publishing a Privacy Act system of records notice describing records in the ''Office of Intelligence and Analysis Enterprise Records System, DHS/IA–001'' (ERS). These records were previously covered by the Department of Homeland Security, Homeland Security Operations Center (HSOC) Database [DHS/IAIP–001], last published on April 18, 2005 [70 FR 20156]. The DHS/IAIP–001 SORN originally addressed the treatment of Privacy Act records under the administrative and organizational framework of the former DHS Information Analysis and Infrastructure Protection (IAIP) Directorate.

After successive organizational realignments of the Department by the Secretary and Congress, in 2005 and 2006 respectively, the IAIP Directorate was effectively eliminated and the functional responsibilities and organization of what was then IAIP's Office of Information Analysis, today the Office of Intelligence and Analysis (I&A), were elevated when I&A became a stand alone organization within the Department, headed by what is now the position of Under Secretary for I&A, with direct-report responsibilities to the Secretary. Thus, ERS replaces those aspects of the HSOC Database [DHS/IAIP–001] SORN insofar as they previously applied to I&A records, but does not rescind, revoke, or supersede any portion of the previously published HSOC Database SORN, itself, insofar as it continues to apply to other components of DHS who maintain records within and consistent with that system.

ERS is a system of records established pursuant to the Homeland Security Act of 2002 (Pub. L. 107–296), as amended, and subject to the Privacy Act of 1974, 5 U.S.C. 552a, to support both the mission of I&A in providing intelligence and analysis support directly to DHS leadership; to all DHS operational components, elements, and other offices and activities; and to the Under Secretary for I&A, as Chief Intelligence Officer of the Department, in his role of effectively integrating and managing DHS's Intelligence Programs. I&A is the DHS-wide analytic entity and unified intelligence office which directly supports the Under Secretary for I&A, other DHS elements responsible for carrying out the mission of the Department under the Homeland Security Act of 2002, as amended, and other federal, State, local, tribal, and private sector DHS partners with responsibilities for securing the homeland from natural and manmade threats. As a member of the National Intelligence Community, I&A is also obligated to conduct its mission in conformance with the requirements of Executive Order 12333, as amended, ''United States Intelligence Activities,'' dated December 4, 1981. Amongst other requirements, Section 2.3 of Executive Order 12333 requires that each agency head within the IC establish procedures to govern the collection, retention, and dissemination of information concerning U.S. Persons, in a manner which protects the privacy and Constitutional rights of those U.S. Persons.

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 personally identifiable information. 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. Individuals may request their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR part 5. The Privacy Act requires each agency to publish in the **Federal Register** a description of 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 regarding the uses to which personally identifiable information is put, and to assist individuals to more easily find such files within the agency. Pursuant to his statutory authorities under section 222 of the Homeland Security Act of 2002, Public Law 107–296, section 222, 116 Stat. 2135, 2155, the DHS Chief Privacy Officer is the senior DHS official appointed by the Secretary to oversee implementation of the Privacy Act within the Department and to undertake other privacy-related activities. Accordingly, the DHS Chief Privacy Officer published the system of records notice which corresponds with this proposed rule.

The Privacy Act also allows government agencies, as appropriate, to exempt certain records from the access and amendment provisions. Where an agency seeks to claim an exemption, however, it must issue a Notice of Proposed Rulemaking to make clear to the public the reasons why a particular exemption is claimed. DHS is claiming exemptions from certain requirements of the Privacy Act by publication of this proposed rule.

Accordingly, DHS proposes to exempt this system, in part, from certain provisions of the Privacy Act and to add that exemption to Appendix C to Part 5, DHS Systems of Records Exempt from the Privacy Act. I&A needs these exemptions in order to protect information relating to authorized intelligence, counterterrorism, homeland security, and related law enforcement activities from disclosure to subjects of investigations and others who, by accessing or knowing this information, could interfere with those activities or otherwise place in jeopardy the national or homeland security. Specifically, the exemptions are necessary in order to prevent revealing information concerning intelligence, counterterrorism, homeland security, or related investigative efforts. Revealing such information to the subject or other individual could reasonably be expected to compromise ongoing efforts of the Department to identify, understand, analyze, investigate, and counter the activities that threaten national or homeland security; compromise classified or other sensitive information; 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, and interfere with intelligence or law enforcement analytic or investigative processes; or constitute a potential danger to the health or safety of intelligence, counterterrorism, homeland security, and law enforcement personnel, confidential sources and informants, or potential witnesses.

The exemptions proposed here are standard law enforcement and national security exemptions exercised by a large number of federal law enforcement and intelligence agencies. In appropriate circumstances, where compliance would not appear to interfere with or adversely affect the national or homeland security of the United States, or the law enforcement purposes of any investigatory material contained within this system, the applicable exemptions may be waived.

List of Subjects in 6 CFR Part 5

Classified information, Privacy, Courts; Freedom of information; Government employees.

For the reasons stated in the preamble and pursuant to the authority vested in the Department of Homeland Security by 5 U.S.C. 552a, and assigned to me under Section 222 of the Homeland Security Act of 2002, DHS proposes to amend 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 section 8:

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

* * * * *

8. DHS/IA–001, Enterprise Records System.

(a) Pursuant to 5 U.S.C. 552a(k)(1), (2), (3), and (5), this system of records is exempt from 5 U.S.C. 552a(c)(3), (d)(1), (2), (3), (4), and (5), (e)(1), (e)(4)(G), (H), and (I), and (f). 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 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.

(3) 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 ERS 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 I&A 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 ERS may be less than fully clear, DHS will only disclose such records after determining whether such disclosures are themselves consistent with the published ERS routine uses. Moreover, it should be noted that, as concerns the receipt by I&A, 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 I&A pursuant to that Executive Order. Specifically, I&A intelligence personnel may acquire information which identifies a particular U.S. Person, retain it within or disseminate it from ERS, as appropriate, only when it is determined that the personally identifying information is necessary for the conduct of I&A's functions, and otherwise falls into one of a limited number of authorized categories, 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.

(4) From subsections (e)(4) (G), (H) and (I) (Access), and (f) (Agency Rules), inasmuch as it is unnecessary for the publication of rules and procedures contemplated therein since the ERS, pursuant to subsections (1) and (2), 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 ERS, 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.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–10891 Filed 5–14–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

6 CFR Part 5

[Docket No. DHS–2008–0003]

Privacy Act of 1974: Implementation of Exemptions; Law Enforcement Information Database (LEIDB)/ Pathfinder

AGENCY: Privacy Office, Office of the Secretary, DHS.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security is giving concurrent notice of a system of records pursuant to the Privacy Act of 1974 for the United States Coast Guard's Law Enforcement Information Data Base (LEIDB)/ Pathfinder system. In this proposed rulemaking, the Department proposes to exempt this system of records from one or more provisions of the Privacy Act because of criminal, civil, intelligence and administrative enforcement requirements.