Proposed Rules

Federal Register
Vol. 70, No. 73
Monday, April 18, 2005

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

6 CFR Part 5, Appendix C

[DHS–2005–0029]

Privacy Act of 1974: Implementation of Exemptions: the Homeland Security Operations Center Database

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security is concurrently establishing one new system of records pursuant to the Privacy Act of 1974, the Homeland Security Operations Center Database. In this proposed rulemaking, the Department of Homeland Security proposes to exempt portions of this system of records from one or more provisions of the Privacy Act because of criminal, civil and administrative enforcement requirements.

DATES: Comments must be received on or before May 18, 2005.

ADDRESSES: You may submit comments, identified by docket number DHS–2004–, by one of the following methods:

- EPA Federal Partner EDOCKET Web site: *http://www.epa.gov/feddocket*. Follow instructions for submitting comments on the Web site.
- DHS has joined the Environmental Protection Agency (EPA) online public docket and comment system on its Partner Electronic Docket System (Partner EDOCKET).
- Federal eRulemaking Portal: *http://www.regulations.gov*. Follow the instructions for submitting comments.
- Fax: (202) 772–5036 (This is not a toll-free number).
- Mail: Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security, Nuala O'Connor Kelly, DHS Chief Privacy Officer, Washington, DC 20528.
- Hand Delivery/Courier: Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security, Nuala O'Connor Kelly, Chief Privacy Officer, 245 Murray Lane, SW., Building 410, Washington, DC 20528, 7:30 a.m. to 4 p.m.

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.epa.gov/feddocket*, including any personal information provided. For detailed instructions on submitting comments and additional information on the rulemaking process, see the ''Public Participation'' heading of the **SUPPLEMENTARY INFORMATION** section of this document.

Docket: For access to the docket to read background documents or comments received, go to *http://www.epa.gov/feddocket*. You may also access the Federal eRulemaking Portal at *http://www.regulations.gov*.

FOR FURTHER INFORMATION CONTACT: Sandy Ford Page, Director, Disclosure Officer, Office of the Chief of Staff, Office of the Undersecretary for Information Analysis and Infrastructure Protection, Department of Homeland Security, Washington, DC 20528 by telephone (202) 282–8522 or facsimile (202) 282–9069; Nuala O'Connor Kelly, DHS Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528, by telephone (202) 772–9848 or facsimile (202) 772–5036.

SUPPLEMENTARY INFORMATION:

Background

Concurrently with the publication of this notice of proposed rulemaking, the Department of Homeland Security (DHS) is publishing a Notice establishing a new system of records that is subject to the Privacy Act of 1974, 5 U.S.C. 552a. DHS is proposing to exempt this system in part, from certain provisions of the Privacy Act. This system is the Office of the Undersecretary for Information Analysis and Infrastructure Protection (IAIP) Homeland Security Operations Center (HSOC) Database (DHS/IAIP001), which is being established to serve as the primary national-level hub for operational communications and information pertaining to domestic incident management and serves as the Nation's single point of threat information integration and dissemination to secure the homeland. The HSOC Database will support a single, centralized repository for gathered information.

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 Homeland Security Act of 2002 requires the Secretary of DHS to appoint a senior official to oversee implementation of the Privacy Act and to undertake other privacy-related activities. Pub. L. 107–296, § 222, 116 Stat. 2135, 2155 (Nov. 25, 2002) (HSA). The systems of records being published today help to carry out the DHS Chief Privacy Officer's statutory activities.

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. By separate notice, the Department has described the Homeland Security Operations Center database.

The Privacy Act allows government agencies to exempt certain records from the access and amendment provisions. If an agency claims 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 exemption from certain requirements of the Privacy Act. In the case of DHS/IAIP 001, which consists of operational communications and information pertaining to domestic incident management, allowing access to the

information that is derived from these files could alert the subject of the information to an investigation of an actual or potential criminal, civil, or regulatory violation and reveal investigative interest on the part of DHS or another agency. Disclosure of the information would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the information would also permit the individual who is the subject of a record to impede the investigation and avoid detection or apprehension, which undermines the entire system. This exemption is standard law enforcement and national security exemption utilized by numerous law enforcement and intelligence agencies.

List of Subjects in 6 CFR Part 5

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

For the reasons stated in the preamble, 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. Subpart B also issued under 5 U.S.C. 552a.

2. Add at the end of Appendix C the following:

* * * * *

DHS/IAIP/OO1

Portions of the following DHS systems of records are exempt from certain provisions of the Privacy Act pursuant to 5 U.S.C. 552(j) and (k): DHS/IAIP 001, Department of Homeland Security (DHS) Homeland Security Operations Center database allows IAIP to maintain and retrieve intelligence information and other information received from agencies and components of the Federal Government, foreign governments, organizations or entities, international organizations, state and local government agencies (including law enforcement agencies), and private sector entities, as well as information provided by individuals, regardless of the medium used to submit the information or the agency to which it was submitted. This system also contains: information regarding persons on watch lists with possible links to terrorism; the results of intelligence analysis and reporting; ongoing law enforcement investigative information, information systems security analysis and reporting; historical law enforcement information, operational and administrative records; financial information; and public-source data such as that contained in media reports and commercial databases as appropriate to identify and assess the nature and scope of terrorist threats to the homeland, detect and identify threats of terrorism against the United States, and understand such threats in light of actual and potential vulnerabilities of the homeland. Data about the providers of information, including the means of transmission of the data is also retained.

IAIP will use the information in the HSOC database to access, receive, and analyze law enforcement information, intelligence information, and other information and to integrate such information in order identify and assess the nature and scope of terrorist or other threats to the homeland.

Pursuant to exemptions (j)(2), (k)(1), and (k)(2) of the Privacy Act, portions of this system are exempt from 5 U.S.C. 552a(c)(3); (d); (e)(1); (e)(4)(G), (H) and (I), and (e)(8), (f), and (g). Exemptions from the particular subsections are justified, on a case by case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c) (3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation and avoid detection or apprehension, which undermines the entire system.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation and reveal investigative interest on the part of DHS or another agency. Access to the records would permit the individual who is the subject of a record to impede the investigation and avoid detection or apprehension. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated. The information contained in the system may also include properly classified information, the release of which would pose a threat to national defense and/or foreign policy. In addition, permitting access and amendment to such information also could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e) (1) (Relevancy and Necessity of Information) because in the course of operations DHS IAIP must be able to review information from a variety of sources. What information is relevant and necessary may not always be apparent until after the evaluation is completed. In the interests of Homeland Security, it is appropriate to include a broad range of information that may aid in identifying and assessing the nature and scope of terrorist or other threats to the Homeland. Additionally, investigations into potential violations of federal law, the accuracy of information obtained or introduced, occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective enforcement of federal laws, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e) (4) (G), (H) and (I) (Agency Requirements), and (f), because portions of this system are exempt from the access and amendment provisions of subsection (d).

Dated: April 7, 2005.

Nuala O'Connor Kelly,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 05–7705 Filed 4–15–05; 8:45 am]

BILLING CODE 4410–10–P

NUCLEAR REGULATORY COMMISSION

10 CFR Part 52

RIN 3150–AH56

AP1000 Design Certification

AGENCY: Nuclear Regulatory Commission.

ACTION: Proposed rule.

SUMMARY: The Nuclear Regulatory Commission (NRC or Commission) proposes to amend its regulations to certify the AP1000 standard plant design. This action is necessary so that applicants or licensees intending to construct and operate an AP1000 design may do so by referencing the AP1000