Dated: December 22, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E9–933 Filed 1–15–09; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2008–0118]

Privacy Act of 1974; Department of Homeland Security—024 Facility and Perimeter Access Control and Visitor Management System of Records

AGENCY: Privacy Office; DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974 and as part of the Department of Homeland Security's ongoing effort to review and update legacy system of record notices, the Department of Homeland Security proposes to consolidate into a new Department of Homeland Security system of records notice titled, DHS/All—024 Facility and Perimeter Access Control and Visitor Management System of Records: Treasury/CS.081 Dock Passes, October 18, 2001, Justice/INS–014 Security Access Control System, January 22, 2001, and to partially consolidate DHS/OS–001 Office of Security File System, September 12, 2006, and FEMA/SEC–1 Security Support System, September 7, 1990. Categories of individuals, categories of records, and the routine uses of this legacy system have been reviewed and updated to better reflect the Department's facility and perimeter access control and visitor management record system. Additionally, the Department of Homeland Security is issuing a Notice of Proposed Rulemaking concurrent with this system of records elsewhere in the **Federal Register**. The activities performed by the Department's Facility and Perimeter Access Control and Visitor Management systems often overlap with other security-related activities. Accordingly, data within each of the categories of individuals, categories of records, and routine uses may have similarities with other security-related systems of records, but each system is distinct based on its purpose. Further, this system of records is separate from DHS-OS–2006–047 Personal Identify Verification Management System which supports the administration of the HSPD–12 program that directs the use of a common identification credential for both logical and physical access to federally controlled facilities and information systems while enhancing security, increasing efficiency, identifying and reducing fraud, and protecting personally identifiable information.

Records within this system apply only to perimeters and facilities where access is controlled by the Department of Homeland Security. This system of records does not apply to (1) facilities where the Department's components or offices have a presence but where the General Services Administration has an established contract for security services or (2) facilities where Immigration and Custom Enforcement's Federal Protective Service provides oversight on the contract.

Exclusion is made to perimeters and facilities secured by the United States Secret Service pursuant to 18 U.S.C. 3056 and 3056A and are not included under this system of records. This consolidated system will be included in the DHS inventory of record systems.

DATES: Written comments must be submitted on or before February 17, 2009. This new system will be effective February 17, 2009.

ADDRESSES: You may submit comments, identified by docket number DHS–2008–0118 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov*. Follow the instructions for submitting comments.
- *Fax*: 703–483–2999.
- *Mail*: Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.
- *Instructions*: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change and may be read at *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*.

FOR FURTHER INFORMATION CONTACT: For general questions and privacy issues please contact: Hugo Teufel III (703–235–0780), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

Pursuant to the savings clause in the Homeland Security Act of 2002, Public Law 107–296, Section 1512, 116 Stat. 2310 (November 25, 2002), the Department of Homeland Security (DHS) and its components and offices have relied on preexisting Privacy Act systems of records notices for the collection and maintenance of records that pertain to facility and perimeter access control and visitor management.

As part of its efforts to streamline and consolidate its Privacy Act record systems, DHS is establishing a new agency-wide system of records under the Privacy Act (5 U.S.C. 552a) for DHS facility and perimeter access control and visitor management records. The facility and perimeter access control and visitor management system of records is the baseline system for facility and perimeter access control and visitor management, as led by the DHS Office of the Chief Security Officer. This will ensure that all components of DHS follow the same privacy rules for collecting and handling access control and visitor management records.

In accordance with the Privacy Act of 1974 and as part of the Department of Homeland Security's ongoing effort to review and update legacy system of record notices, the Department of Homeland Security proposes to consolidate Treasury/CS.081 Dock Passes, October 18, 2001, Justice/INS–014 Security Access Control System, January 22, 2001, and to partially consolidate DHS/OS–001 Office of Security File System, September 12, 2006, and FEMA/SEC–1 Security Support System (55 FR 37182), into a new Department of Homeland Security system of records notice titled, DHS/All—024 Facility and Perimeter Access Control and Visitor Management System of Records. Categories of individuals, categories of records, and the routine uses of this legacy system have been reviewed and updated to better reflect the Department's facility and perimeter access control and visitor management record system.

The activities performed by the Department's Facility and Perimeter Access Control and Visitor Management systems often overlap with other security-related activities. Accordingly, data within each of the categories of individuals, categories of records, and routine uses may have similarities with other security-related systems of records, but each system is distinct based on its purpose.

Records within this system apply only to perimeters and facilities where access is controlled by the Department of Homeland Security. This system of records does not apply to (1) facilities where the Department's components or offices have a presence but where the General Services Administration has an established contract for security services

or (2) facilities where Immigration and Custom Enforcement's Federal Protective Service provides oversight on the contract.

Further, this system of records is separate from DHS–OS–2006–047 Personal Identify Verification Management System which supports the administration of the HSPD–12 program that directs the use of a common identification credential for both logical and physical access to federally controlled facilities and information systems while enhancing security, increasing efficiency, identifying and reducing fraud, and protecting personally identifiable information.

Additionally, the Department of Homeland Security is issuing a Notice of Proposed Rulemaking concurrent with this system of records elsewhere in the **Federal Register**. Exclusion is made to perimeters and facilities secured by the United States Secret Service pursuant to 18 U.S.C. 3056 and 3056A and are not included under this system of records. This consolidated system will be included in the DHS inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses and disseminates individual's records. The Privacy Act applies to information that is maintained in a ''system of records.'' A ''system of records'' is a group of any records under the control of an agency from which information is stored and retrieved by the name of the individual or by some identifying number such as property address, mailing address, or symbol assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. DHS extends administrative Privacy Act protections to all individuals where information is maintained on both U.S. citizens, lawful permanent residents, and visitors. 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 5.21.

The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses of their records, and to assist individuals to more easily find such files within the agency. Below is a description of the Visitor Management and Access Control System of Records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this new system of records to the Office of Management and Budget (OMB) and to Congress.

SYSTEM OF RECORDS:

DHS/ALL–024.

SYSTEM NAME:

Department of Homeland Security—024 Facility and Perimeter Access Control and Visitor Management System of Records

SECURITY CLASSIFICATION:

Unclassified, sensitive, for official use only, and classified.

SYSTEM LOCATION:

Records are maintained at several Headquarters locations and in component offices of the Department of Homeland Security, in both Washington, D.C. and field locations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include: (1) Any employee, contractor, consultant, intern, fellow, or others with regular access and an access control pass which grants unescorted access to a DHS facility or information technology system and any visitor to a DHS facility; (2) violators of DHS access or perimeter control; (3) applicants for employment, contractors, or those needing unescorted access to DHS facilities or information technology systems; (4) State and local government personnel and private-sector individuals who serve on an advisory committee and board sponsored by DHS; (5) individuals, including State and local government personnel and private-sector individuals, who are authorized by DHS to access Departmental facilities, including classified facilities, communications security equipment, and information technology systems that process national or homeland security classified information; (6) individuals accused of security violations or found in violation.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records covered by this system include:

- Individual's full name;
- Organization's name;
- Social security number;
- Date of birth;
- Citizenship;
- Country of origin, if applicable;
- Telephone number;
- Physical descriptions;
- Biometric information;
- Photograph;
- Visitor badge number, if applicable;
- Date and time of entry and departure;
- Driver's license and other form of identification information;
- License plate number and state of issuance;
- Make and model of vehicle;
- Reports, files, records received from other Federal agencies;
- Records relating to management and operation of DHS programs to safeguard classified and sensitive but unclassified information, including but not limited to:
  - Document control registries;
  - Courier authorization requests;
  - Non-disclosure agreements;
  - Records of security violations;
  - Records of document transmittals; and
  - Requests for secure storage and communications equipment.
- Records relating to the management and operation of the DHS security program, including but not limited to:
  - Inquiries relating to suspected security violation(s);
  - Recommended remedial actions for possible security violation(s);
  - Reports of investigation regarding security violations;
  - Statements of individuals;
  - Affidavits; and
  - Correspondence.
- Records relating to the management and operation of the Office of Security's facility and perimeter access control and visitor management system including but not limited to:
  - Facility and perimeter access registries;
  - Courier cards;
  - Access control card requests; and
  - Specific information from standard DHS forms used to conduct criminal history record checks; and
  - Closed circuit television (CCTV) systems and recordings.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; the Federal Records Act, 6 U.S.C., the Homeland Security Act; 44 U.S.C. 3101; and Executive Order 9397; Executive Order 12968, Federal Property Regulations, issued July 2002.

PURPOSE(S):

The purpose of this system is to maintain records associated with DHS facility and perimeter access control, including access to DHS Information Technology and access to classified facilities, as well as visitor management.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records of information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (including United States Attorney Offices) or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. Any employee of DHS in his/her official capacity;

3. Any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the written request of the individual to whom the record pertains.

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

D. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) or harm to the individual who relies upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To an appropriate Federal, State, local, tribal, foreign, or international agency or contract provider, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee or contractor, the issuance of a security clearance, the reporting of an investigation of an employee or contractor, the letting of a contract, or the issuance of a license, grant or other benefit and disclosure is appropriate to the proper performance of the official duties of the person making the request.

I. To a public or professional licensing organization when such information indicates, either by itself or in combination with other information, a violation or potential violation of professional standards, or reflects on the moral, educational, or professional qualifications of an individual who is licensed or who is seeking to become licensed.

J. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

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

STORAGE:

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on servers, magnetic disc, tape, digital media, and CD–ROM.

RETRIEVABILITY:

Records may be retrieved by individual name, date of birth, and social security number, if applicable.

SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RETENTION AND DISPOSAL:

Pursuant to GRS 18, Item 22a personnel security clearance files are destroyed upon notification of death or not later than five years after separation or transfer of employee or no later than five years after contract relationship expires, whichever is applicable.

Pursuant to GRS 18, Item 6 requests and authorizations for individuals to have access to classified files are destroyed two years after authorization expires.

Pursuant to GRS 11, Item 4a identification credentials including cards, badges, parking permits, photographs, agency permits to operate motor vehicles, and property, dining room and visitors passes, and other identification credentials are destroyed credentials three months after return to issuing office.

Pursuant to GRS 18, Item 17 registers or logs used to record names of outside contractors, service personnel, visitors, employees admitted to areas, and reports on automobiles and passengers for areas under maximum security are destroyed five years after final entry or five years after date of document, as appropriate.

Other documents pursuant to GRS 18, Item 17b are destroyed two years after final entry or two years after date of document, as appropriate.

Where records are used as evidence in an investigation or in an administrative, litigation, or other proceeding, the records will be retained until final disposition of the investigation or proceeding.

SYSTEM MANAGER AND ADDRESS:

For Headquarters components of DHS, the System Manager is the Director of Departmental Disclosure, Department of Homeland Security, Washington, DC 20528. For components of DHS, the System Manager can be found at *http://www.dhs.gov/foia* under ''contacts.''

NOTIFICATION PROCEDURE:

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Headquarters or component's FOIA Officer, whose contact information can be found at *http://www.dhs.gov/foia* under ''contacts.'' If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, SW., Building 410, STOP–0550, Washington, DC 20528.

When seeking records about yourself from this system of records or any other Departmental, system of records your request must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, *http://www.dhs.gov* or 1–866–431–0486. In addition, you should provide the following:

- An explanation of why you believe the Department would have information on you,
- Identify which component(s) of the Department you believe may have the information about you,
- Specify when you believe the records would have been created,
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records,
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

RECORD ACCESS PROCEDURES:

See ''Notification procedure'' above.

CONTESTING RECORD PROCEDURES:

See ''Notification procedure'' above.

RECORD SOURCE CATEGORIES:

Records are generated from sources contacted during visits to Department facilities.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Secretary of Homeland Security has exempted this system from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), (I), and (f) of the Privacy Act pursuant to 5 U.S.C. 552a (k)(1), (k)(2), and (k)(5) of the Privacy Act.

Dated: December 22, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E9–928 Filed 1–15–09; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2008–0120]

Privacy Act of 1974; Department of Homeland Security—023 Personnel Security Management System of Records

AGENCY: Privacy Office; DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974 and as part of the Department of Homeland Security's ongoing effort to review and update system of records notices, the Department of Homeland Security proposes to consolidate into a new Department of Homeland Security system of records notice titled, Personnel Security Management System of Records: Treasury/CS.270 Background-Record File of Non-Customs Employees, Treasury/CS.284 Personnel Verification System, and DOT/CG 611 Investigative Case System, and partially consolidate DHS/OS–001 Office of Security File System and FEMA/SEC–1 Security Support System. Categories of individuals, categories of records, and the routine uses of these legacy systems have been reviewed and updated to better reflect the Department's personnel security management record system. Additionally, the Department of Homeland Security is issuing a Notice of Proposed Rulemaking concurrent with this system of records elsewhere in the **Federal Register**. The activities performed by the Department's Personnel Security program often overlap with other security-related activities such as access control and investigatory records. Accordingly, data within each of the categories of individuals, categories of records, and routine uses may have similarities with other security-related systems of records, but each system is distinct based on its purpose. This consolidated system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Written comments must be submitted on or before February 17, 2009. This new system will be effective February 17, 2009.

ADDRESSES: You may submit comments, identified by docket number DHS–2008–0120 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Fax:* 703–483–2999.
- *Mail:* Hugo Teufel III, Chief Privacy Officer, Privacy Office, 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 and may be read at *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.*

FOR FURTHER INFORMATION CONTACT: For general questions and privacy issues