[Federal Register: September 29, 2009 (Volume 74, Number 187)]

[Notices]

[Page 49882-49885]

From the Federal Register Online via GPO Access [wais.access.gpo.gov]

[DOCID:fr29se09-64]

=======================================================================

-----------------------------------------------------------------------

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2009-0038]

Privacy Act of 1974; Department of Homeland Security/ALL-004

General Information Technology Access Account Records System of Records

AGENCY: Privacy Office; DHS.

ACTION: Notice of Privacy Act system of records update.

-----------------------------------------------------------------------

SUMMARY: In accordance with the Privacy Act of 1974 the Department of

Homeland Security proposes to update and reissue a Department of

Homeland Security system of records notice titled, Department of

Homeland Security/ALL-004 General Information Technology Access Account

Records System of Records. As a result of the biennial review of this

system, the Department proposes to include the addition of social

security numbers in the categories of records covered by the system for

the purpose of identifying an individual for system access.

Additionally, a new routine use has been added for the purpose of

sharing with the media where appropriate. This updated system will be

included in the Department of Homeland Security's inventory of record

systems.

DATES: Written comments must be submitted on or before October 29,

2009.

ADDRESSES: You may submit comments, identified by Docket Number DHS-

2009-0038 by one of the following methods:

Federal e-Rulemaking Portal: <http://frwebgate.access.gpo.gov/cgi-bin/leaving.cgi?from=leavingFR.html&log=linklog&to=http://www.regulations.gov>.

Follow the instructions for submitting comments.

Fax: 703-483-2999.

Mail: Mary Ellen Callahan, 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 to <http://frwebgate.access.gpo.gov/cgi-bin/leaving.cgi?from=leavingFR.html&log=linklog&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://frwebgate.access.gpo.gov/cgi-bin/leaving.cgi?from=leavingFR.html&log=linklog&to=http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: For general questions and for privacy

issues please contact: Mary Ellen Callahan (703-235-0780), Chief

Privacy Officer, Privacy Office, U.S. Department of Homeland Security,

Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

As part of its efforts to maintain its Privacy Act record systems,

the Department of Homeland Security (DHS) is updating and reissuing a

Department-wide system of records under the Privacy Act (5 U.S.C. 552a)

for DHS/ALL-004 General Information Technology Access Account Records

System of Records (73 FR 28139, May 15, 2008). This will ensure that

all components of DHS follow the same privacy rules for collecting and

handling information technology access account records. The collection

and maintenance of this information will assist DHS in managing the

Department's information technology access account records.

This system of records is part of DHS' ongoing record integration

and management efforts. This system consists of information collected

in order to provide authorized individuals with access to DHS

information technology resources. This information includes user name,

business affiliation, account information and passwords.

In accordance with the Privacy Act of 1974, DHS is giving notice

that it proposes to update and reissue a DHS system of records notice

titled, DHS/ALL-004 General Information Technology Access Account

Records System of Records. As a result of the biennial review of this

system, the

[[Page 49883]]

Department proposes to include the addition of social security numbers

in the categories of records covered by the system for the purpose of

identifying an individual for system access. Additionally, a new

routine use has been added for the purpose of sharing with the media

where appropriate. This updated system will be included in DHS's

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 individuals' 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 for which information is retrieved by the name of

an individual or by some identifying number, symbol, or other

identifying particular assigned to the individual. In the Privacy Act,

an individual is defined to encompass United States citizens and lawful

permanent residents. As a matter of policy, DHS extends administrative

Privacy Act protections to all individuals where systems of records

maintain information on U.S. citizens, lawful permanent residents, and

visitors. Individuals may request access to 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 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 to

which their records are put, and to assist individuals to more easily

find such files within the agency. Below is the description of DHS/ALL-

004 General Information Technology Access Account Records System of

Records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of

this system of records to the Office of Management and Budget and to

Congress.

SYSTEM OF RECORDS:

DHS/ALL-004.

SYSTEM NAME:

Department of Homeland Security General Information Technology

Access Account Records System of Records.

SECURITY CLASSIFICATION:

Sensitive but unclassified.

SYSTEM LOCATION:

Records are maintained at several Headquarters locations and in

component offices of the Department of Homeland Security, in both

Washington, DC and field locations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include:

All persons who are authorized to access DHS information technology

resources, including employees, contractors, grantees, private

enterprises and any lawfully designated representative of the above and

including representatives of Federal, State, territorial, tribal,

local, international, or foreign government agencies or entities, in

furtherance of the DHS mission. Also covered by this system are

individuals who serve on DHS boards and committees; individuals who

have business with DHS and who have provided personal information in

order to facilitate access to DHS information technology resources; and

individuals who are points of contact provided for government business,

operations, or programs, and the individual(s) they list as emergency

contacts.

CATEGORIES OF RECORDS IN THE SYSTEM:

Name;

Social Security Number;

Business and affiliations;

Facility positions held;

Business telephone numbers;

Cellular phone numbers;

Pager numbers;

Numbers where individuals can be reached while on travel

or otherwise away from the office;

Citizenship;

Level of access;

Home addresses;

Electronic mail addresses of senders and recipients;

Records on access to DHS computers and networks including

user ID and passwords;

Date and time of access;

IP address of access;

Logs of internet activity and records on the

authentication of the access request;

Records on the names and phone numbers of other contacts;

and

Positions or titles of contacts, their business/

organizational affiliations and other contact information provided to

the Department that is derived from other sources to facilitate

authorized access to DHS Information Technology resources.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; 44 U.S.C. 3101; and EO 9397 (SSN).

PURPOSE(S):

This system will collect a discreet set of personally identifiable

information in order to provide authorized individuals access to or

interact with DHS information technology resources. The information

collected by the system will include full name, user name, account

information, citizenship, business/organizational affiliation, contact

information, and passwords. Directly resulting from the use of DHS

information technology resources is the collection, review, and

maintenance of any logs, audits, or other such security data regarding

the use of such information technology resources.

The system enables DHS to maintain: Account information required

for approved access to information technology; lists of individuals who

are appropriate organizational points of contact; and lists of

individuals who are emergency points of contact. The system will also

enable DHS to provide individuals access to certain programs and

meeting attendance and where appropriate allow for sharing of

information between individuals in the same operational program to

facilitate collaboration.

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 or

information contained in this system may be disclosed outside DHS as a

routine use pursuant to 5 U.S.C. 552a(b)(3), limited by privacy impact

assessments, data sharing, or other agreements, 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

[[Page 49884]]

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

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 Sec. 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 that rely 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 sponsors, employers, contractors, facility operators,

grantees, experts, and consultants in connection with establishing an

access account for an individual or maintaining appropriate points of

contact and when necessary to accomplish a DHS mission function or

objective related to this system of records.

I. To other individuals in the same operational program supported

by an information technology system, where appropriate notice to the

individual has been made that his or her contact information will be

shared with other members of the same operational program in order to

facilitate collaboration.

J. To Federal agencies such as Office of Personnel Management, the

Merit Systems Protection Board, the Office of Management and Budget,

Federal Labor Relations Authority, Government Accountability Office,

and the Equal Employment Opportunity Commission in the fulfillment of

these agencies' official duties.

K. To international, Federal, State and local, tribal, private and/

or corporate entities for the purpose of the regular exchange of

business contact information in order to facilitate collaboration for

official business.

L. To appropriate agencies, entities, and persons when: It is

suspected or confirmed that the security or confidentiality of

information in the system of records has been compromised; DHS 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) that rely upon the compromised information; and the

disclosure is made to such agencies, entities, and persons who are

reasonably necessary to assist in DHS's efforts to respond to the

suspected or confirmed compromise and prevent, minimize, or remedy such

harm.

M. 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 on paper and/or in digital or other

electronic form. Digital and other electronic images are stored on a

storage area network in a secured environment. Records, whether paper

or electronic, may be stored at the DHS Headquarters or at the

component level.

RETRIEVABILITY:

Information may be retrieved, sorted, and/or searched by an

identification number assigned by computer, social security number, by

facility, by business affiliation, e-mail address, or by the name of

the individual, or other employee data fields previously identified in

this SORN.

SAFEGUARDS:

Information in this system is safeguarded in accordance with

applicable laws, rules and policies, including the DHS Information

Technology Security Program Handbook and DHS Information Security

Program Policy and Handbook. Further, Department of Homeland Security/

ALL-004 General Information Technology Access Account Records system of

records security protocols will meet multiple National Institute of

Standards and Technology (NIST) Security Standards from Authentication

to Certification and Accreditation. Records in the Department of

Homeland Security/ALL-004 General Information Technology Access Account

Records system of records will be maintained in a secure, password

protected electronic system that will utilize security hardware and

software to include: multiple firewalls, active intruder detection, and

role-based access controls. Additional safeguards will vary by

component and program. All records are protected from unauthorized

access through appropriate administrative, physical, and technical

safeguards. These safeguards include: restricting access to authorized

personnel who have a ``need to know;'' using locks; and password

protection identification features. Classified information is

appropriately stored in accordance with applicable requirements. DHS

file areas are locked

[[Page 49885]]

after normal duty hours and the facilities are protected from the

outside by security personnel.

RETENTION AND DISPOSAL:

Records are securely retained and disposed of in accordance with

the National Archives and Records Administration's General Records

Schedule 24, section 6, ``User Identification, Profiles,

Authorizations, and Password Files.'' Inactive records will be

destroyed or deleted 6 years after the user account is terminated or

password is altered, or when no longer needed for investigative or

security purposes, whichever is later.

SYSTEM MANAGER AND ADDRESS:

For Headquarters and components of DHS, the System Manager is the

Chief Privacy Officer and Chief Freedom of Information Act Officer,

Privacy Office, Department of Homeland Security, Washington, DC 20528.

For components of DHS, the System Manager can be found at <http://frwebgate.access.gpo.gov/cgi-bin/leaving.cgi?from=leavingFR.html&log=linklog&to=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://frwebgate.access.gpo.gov/cgi-bin/leaving.cgi?from=leavingFR.html&log=linklog&to=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 and

Chief Freedom of Information Act Officer, Privacy Office, Department of

Homeland Security, 245 Murray Drive, SW., Building 410, STOP-0655,

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 Chief Privacy

Officer and Chief Freedom of Information Act Officer, <http://frwebgate.access.gpo.gov/cgi-bin/leaving.cgi?from=leavingFR.html&log=linklog&to=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;

and

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:

A request for access to records in this system may be made by

writing to the System Manager, identified above, in conformance with 6

CFR Part 5, which provides the rules for requesting access to Privacy

Act records maintained by DHS.

CONTESTING RECORD PROCEDURES:

Same as ``Records Access Procedures'' above.

RECORD SOURCE CATEGORIES:

Information contained in this system is obtained from affected

individuals/organizations/facilities, public source data, other

government agencies and/or information already in other DHS records

systems.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: September 23, 2009.

Mary Ellen Callahan

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E9-23513 Filed 9-28-09; 8:45 am]

BILLING CODE 9110-9B-P