[Federal Register Volume 77, Number 228 (Tuesday, November 27, 2012)]

[Notices]

[Pages 70792-70795]

From the Federal Register Online via the Government Publishing Office [[www.gpo.gov](http://www.gpo.gov)]

[FR Doc No: 2012-28675]

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

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2012-0070]

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

General Information Technology Access Account Records System of Records

AGENCY: Privacy Office, Department of Homeland Security.

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 update the categories of individuals

and categories of records covered by the system. Additionally, the

routine uses have been updated with minor clarifications. 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 December 27,

2012.

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

2012-0070 by one of the following methods:

Federal e-Rulemaking Portal: <http://www.regulations.gov>.

Follow the instructions for submitting comments.

Fax: 202-343-4010.

Mail: Jonathan R. Cantor, Acting 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://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 for privacy

issues please contact: Jonathan R. Cantor (202-343-1717), Acting Chief

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

Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the

Department of Homeland Security (DHS) proposes to update and reissue a

current Department-wide system of records titled DHS/ALL-004 General

Information Technology Access Account Records System of Records (73 FR

28139, May 15, 2008). The collection and maintenance of this

information will assist DHS in managing the

[[Page 70793]]

Department's information technology access account records.

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. Passwords are encrypted and used as

part of the log in process for verification of appropriate access.

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 Department proposes to update the categories of

individuals, to include individuals who have been denied or had access

revoked. In addition, the categories of records has been updated to

include such information as voluntary posting of photos for

collaboration purposes, comments posted for collaboration purposes,

training taken, justification for access, and all logs of activity on

the DHS network. Finally, the routine uses have been updated with minor

clarifications. 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 federal government agencies

collect, maintain, use, and disseminate 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 from 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

Department of Homeland Security (DHS)/ALL-004

System name:

DHS/ALL-004 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:

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.

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;

Individuals who are points of contact provided for

government business, operations, or programs, and the individual(s)

they list as emergency contacts;

Individuals who voluntarily join a DHS-owned and operated

web portal for collaboration purposes; and

Individuals who request access but are denied, or who have

had access revoked.

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;

Business addresses;

Electronic mail addresses of senders and recipients;

Justification for access to DHS computers, networks, or

systems;

Verification of training requirements or other

prerequisite requirements for access to DHS computers, networks, or

systems;

Records on access to DHS computers and networks including

user ID and passwords;

Registration numbers or IDs associated with DHS

Information Technology resources;

Date and time of access;

Logs of activity of DHS IT resources;

IP address of access;

Logs of Internet activity; and

Records on the authentication of the access request,

names, phone numbers of other contacts, and positions or business/

organizational affiliations and titles of individuals who can verify

that the individual seeking access has a need to access as well as

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:

44 U.S.C. 3101; EO 9397 (SSN), as amended by EO 13487; and 44

U.S.C. 3534.

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, and allow DHS to

track use of DHS IT resources. 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

[[Page 70794]]

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), 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 relevant or 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.

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 General

Services Administration pursuant to records management inspections

being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency or organization 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 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, email 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, DHS/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 DHS/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

[[Page 70795]]

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 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:

The System Manager is the Chief Information Officer (CIO),

Department of Homeland Security, Washington, DC 20528.

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 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://www.dhs.gov> or 1-866-431-0486. In addition you should:

Explain 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; and

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 the above 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:

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: November 13, 2012.

Jonathan R. Cantor,

Acting Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2012-28675 Filed 11-26-12; 8:45 am]

BILLING CODE 9110-9B-P