[Federal Register Volume 79, Number 154 (Monday, August 11, 2014)]
[Notices]
[Pages 46857-46862]
From the Federal Register Online via the Government Publishing Office [www.gpo.gov]
[FR Doc No: 2014-18703]

---

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2014-0039]

# Privacy Act of 1974; Department of Homeland Security/ALL-037 E-Authentication Records System of Records

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Notice of Privacy Act System of Records.

---

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to establish a new system of records titled, Department of Homeland Security/ALL-037 E-Authentication Records System of Records. This system of records allows the Department of Homeland Security to collect, maintain, and retrieve records about individuals, including members of the public, who electronically authenticate their identities. The information in this system of records includes data collected by programs and applications for use when the Department of Homeland Security or a

[[Page 46858]]

trusted third-party performs some or all of the functions required to enroll, issue, and maintain a credential on DHS's behalf that can be used by an individual to electronically authenticate his or her identity to DHS systems.

These programs and applications include: The Department of Homeland Security's Homeland Security Information Network, which is a trusted network for homeland security mission operations to share sensitive but unclassified information used by federal, state, local, tribal, territorial, international, and private sector homeland security partners to manage operations, analyze data, and send alerts and notices; the U.S. Citizenship and Immigration Services E-Verify Self Check, which is a free service that allows individuals to learn about their work authorization status information; and the U.S. Citizenship and Immigration Services myE-Verify, which is a free service that allows individuals to create an account and access additional features beyond Self Check concerning the use of their personally identifiable information in E-Verify and Self Check such as the ability to lock a Social Security number to prevent its use in E-Verify and Self Check. Additional Department programs or applications may also use third-party authentication.

In addition, the Department of Homeland Security also proposes to consolidate the E-Verify Self Check System of Records (DHS/USCIS-013), last published in the Federal Register on February 16, 2011 (76 FR 9604), into this newly established E-Authentication Records System of Records. As a result of this consolidation, by this notice, DHS intends to remove DHS/USCIS-013 from its inventory of systems of records. The newly established system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Written comments must be submitted on or before September 10, 2014.

ADDRESSES: You may submit comments, identified by Docket Number DHS-2014-0039 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: Karen L. Neuman, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, 245 Murray Drive SW., Building 410, STOP-0655, 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 and privacy related

questions please contact: Karen L. Neuman (202-343-1717), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, 245 Murray Drive SW., Building 410, STOP-0655, 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 establish a new DHS system of records titled, ``DHS/ALL-037 E-Authentication Records System of Records.'' The collection and maintenance of information within this system of records assists DHS in enrolling, issuing, and maintaining credentials (e.g., online accounts) for individuals seeking electronic access to DHS programs, services, and applications, including when DHS uses a trusted third-party identity service provider for these activities. DHS may perform some or all credential management functions (e.g., identity proofing, manage authentication tokens, authenticate users) on its own, choose a single third-party to perform all functions, or use multiple providers for each discrete function. This system of records notice is agnostic as to how DHS applications or systems using electronic authentication wish to engage with third-parties.

DHS has many public-facing programs that provide online access to its services at various levels of assurance, as described in the Office of Management and Budget (OMB) E-Authentication Guidance for Federal Agencies (M-04-04). OMB defines four levels of assurance (LOA), Levels 1 to 4, in terms of the consequences resultant from authentication errors or misuse of credentials. Level 1 is the lowest assurance level, and Level 4 is the highest. For example, an authentication error may occur if an individual gains access to sensitive information he or she is not entitled to access. Depending on the context and the sensitivity of the information accessed, the consequences of such an authentication error could pose significant harm to other individuals and/or to the affected agency. As the consequences of an authentication error become more serious, the required LOA increases.

In order to facilitate access, information must be collected to authenticate an individual's identity at the requisite level of assurance for the purpose of obtaining a credential or electronically authorizing access to a DHS program or application. These programs and applications include: DHS's Homeland Security Information Network (HSIN), which is a trusted network for homeland security mission operations to share sensitive but unclassified information used by federal, state, local, tribal, territorial, international, and private sector homeland security partners to manage operations, analyze data, and send alerts and notices; the U.S. Citizenship and Immigration Services (USCIS) E-Verify Self Check, which is a free service that allows individuals to learn about their work authorization status information; and USCIS myE-Verify, which is a free service that allows individuals to create an account and exercise limited control about the use of their information in E-Verify Self Check. HSIN, E-Verify Self Check, and myE-Verify use trusted third-party identity service providers to perform credential management functions.

Identity proofing is the process by which an identity service provider collects and verifies information (e.g., name, date of birth, Social Security number (SSN), address of residence) about a person for the purpose of issuing credentials to that person. Third-party identity service providers use a variety of verification techniques, including knowledge-based authentication, to generate a quiz containing questions that only the individual should be able to answer. When using the knowledge-based authentication process the third-party identity provider generates a quiz based on commercial identity verification information collected by the third-parties from financial institutions, public records, and other service providers. The information accessed by the third-parties includes information such as the individual's commercial transaction history, mortgage payments, addresses, or past addresses. DHS does not have access to the commercial identity verification information, the quiz questions asked of the individual, or the responses provided thereto; therefore this commercial information is not included in this system of records. Rather, DHS receives assertions (e.g., pass/fail) and assertion references (e.g., transaction ID, date/time of the transaction, and error codes) from the

[[Page 46859]]

identity service provider to facilitate troubleshooting and system management. DHS maintains attributes (e.g., clearances, location, biometrics, and group memberships) collected for identity proofing only when necessary for the DHS program to manage the credential.

DHS may request verified attributes about an individual from the third-party depending on the program or application's requirements. For any attribute DHS requests from the third-party, DHS will ask the user if he or she wishes to share the requested information with DHS prior to gaining access to the DHS online system or application. The user can select to opt-in, meaning he or she will allow DHS access to his or her

attribute information from the third-party in order for him or her to gain access to the DHS system. If the third-party cannot generate a quiz, or if the individual cannot answer the questions provided, the individual may not be able to access program or application.

DHS may share attribute information with trusted third-party identity service providers under contract with DHS or certified by the Federal Identity Management Credential and Access Management (FICAM) initiative for the purpose of authenticating an individual seeking a credential with DHS. More information about FICAM is available at www.idmanagment.gov. Attributes provided to the relying party are limited to: (1) Making authorization decisions; (2) dynamically provisioning accounts; and (3) performing audit logging. The transaction may be included in the individual's credit record as a ``soft inquiry'' that does not impact the individual's credit score when the identity service provider is a credit bureau or uses a credit bureau to conduct identity proofing. The ``soft inquiry'' is not viewable by third parties. DHS may also share attribute information with ``relying parties'' approved by the National Information Exchange Federation (NIEF) Trust Framework Provider who provide federated access to systems. More information about NIEF is available at https://nief.gfipm.net/.

In accordance with the Privacy Act of 1974, DHS is giving notice that it proposes to issue a new DHS system of records notice titled, DHS/ALL-037 E-Authentication Records System of Records. In addition DHS proposes to consolidate the E-Verify Self Check System of Records (DHS/USCIS-013) into this newly-established system of records. As a result of this consolidation, by this notice, DHS intends to remove DHS/USCIS-013 from its inventory of systems of records. This newly established 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 when 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-037 E-Authentication 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-037.

System name:

DHS/ALL-037 E-Authentication Records System of Records.

Security classification:

Sensitive but unclassified.

System location:

Records are maintained at several Headquarters locations and in component offices of DHS, in both Washington, DC, and field locations or by a third-party identity service provider. Records related to identity proofing required for levels of assurance (LOA) 2 and above are also maintained by the third-party identity service provider in accordance with retention requirements identified in the National Institute of Standards and Technology (NIST) Special Publication 800-63 Electronic Authentication Guideline for the applicable LOA.

Categories of individuals covered by the system:

Categories of individuals in this system of records include members of the public, external stakeholders, and federal employees or contractors seeking electronic access to DHS programs and applications. This includes anyone attempting to authenticate his or her identity for the purpose of obtaining a credential to access a DHS program or application electronically, including when the program or application uses a third-party identity service provider to perform some or all

credential management functions (e.g., prove identity, manage authentication tokens, authenticate users).

Categories of records in the system:

Attributes DHS or a third-party identity service provider collects necessary to perform identity proofing at the required level of assurance. Attributes are only retained in this system of records if it is necessary for the program to manage the credential. Examples of attributes collected for identity proofing information include:

- [cir] Name (last, first, middle, and maiden);
- [cir] Date of birth;
- [cir] Place of birth;
- [cir] Financial or utility account number;
- [cir] Address of residence;
- [cir] Social Security number (SSN)--full or partial (may be optional depending on the application);
- [cir] Telephone number--(may be optional depending on the application); and
- [cir] Country of Citizenship.

Assertions and assertion references from a third-party identity service provider such as:

- [cir] Transaction ID;
- [cir] Pass/fail indicator;
- [cir] Date/time of the transaction;
- [cir] Codes associated with the transaction;

Information DHS or third-parties collect necessary to register, issue, and maintain the credential (e.g., to administer multi-factor authentication)

[[Page 46860]]

including verified attributes the identity service provider maintains or passes to DHS after a user successfully passes identity proofing such as:

- [cir] Name;
- [cir] Email addresses;
- [cir] User ID;
- [cir] Passwords;
- [cir] Phone numbers (primary, alternate, mobile, home, work, landline);
- [cir] Two-factor authentication preference (SMS text message, email, phone number for interactive voice response);
- [cir] Self-generated security questions and answers;
- [cir] Level of access;

Credential registration information DHS collects manually that is necessary to perform manual identity verification in cases in which an individual cannot electronically prove his or her identity. Note that some identity proofing information (e.g., copies of government-issued photo identification) is retained in this system of records only if it is necessary for DHS to manage the credential.

Other program-specific attribute information DHS or the identity service provider collects directly on behalf of DHS may include:

- [cir] Citizenship;
- [cir] Accepted Terms of Service (Y/N);
- [cir] Employment information such as job title, job role, organization;
- [cir] Business and affiliations;
- [cir] Faculty positions held;
- [cir] Home addresses;
- [cir] Business addresses;
- [cir] Justification/nomination for access to DHS computers, networks, or systems;
- [cir] Supervisor/nominator's name, job title, organization, phone numbers, email address;
- [cir] Verification of training requirements or other prerequisite requirements for access to DHS computers, networks, or systems;
- [cir] Government-issued identity document type and expiration date;

Records on access to DHS computers, networks, online programs, and applications including user ID and passwords;

- [cir] Registration numbers or IDs associated with DHS Information Technology (IT) resources;
- [cir] Date and time of access;
- [cir] Logs of activity interacting with DHS IT resources;
- [cir] Internet Protocol (IP) address of access;
- [cir] Logs of internet activity; and
- [cir] 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 the system, as well as other contact information provided to the Department or that is derived from other sources to facilitate authorized access to DHS IT resources.

Authority for maintenance of the system:

44 U.S.C. 3101; EO 9397 (SSN), as amended by EO 13487; 44 U.S.C. 3534; Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Public Law (Pub. L.) 104-208, September 30, 1996, Note Section 404. Additional programmatic authorities may apply to maintenance of the credential.

Purpose(s):

This system collects information in order to authenticate an individual's identity for the purpose of obtaining a credential to electronically access a DHS program or application. This system includes DHS programs or applications that use a third-party identity service provider to provide any of the following credential services: Registration, including identity proofing, issuance, authentication, authorization, and maintenance. This system collects information that allows DHS to track the use of programs and applications for system maintenance and troubleshooting. The system also enables DHS to allow an individual to reuse a credential received when applicable and available.

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. Sec. 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. Sec. 552a(b)(3), as follows:

A. To the Department of Justice (DOJ), including Offices of the U.S. Attorneys, 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 or former employee of DHS in his/her official capacity;

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

4. The U.S. 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 (NARA) 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. DHS has determined that as a result of the suspected or confirmed compromise, there is a risk of identity theft or fraud, harm to economic or property interests, harm to an individual, 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

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, when 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

[[Page 46861]]

with establishing, maintaining, or managing an access account for an individual or maintaining appropriate points of contact.

I. To relying parties approved by the National Information Exchange

Federation (NIEF) Trust Framework Provider for the purpose of providing federated access to systems when the user has been provided with appropriate notice and the opportunity to consent. Attributes provided to the relying party are limited to: (1) making authorization decisions; (2) dynamically provisioning accounts; and (3) performing audit logging.

J. 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.

K. To a trusted third-party identity service provider under contract with DHS or certified by the Federal Identity Management Credential and Access Management initiative for the purpose of authenticating an individual seeking a credential with DHS. The information may be included in the individual's credit record as a ``soft inquiry'' that does not impact the individual's credit score when the identity service provider is a credit bureau or uses a credit bureau to conduct identity proofing. The ``soft inquiry'' is not viewable by third parties.

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, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines 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 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, are stored at the DHS Headquarters, at the component level, or at the third-party identity service provider's physical or cloud location.

Retrievability:

Information is retrieved, sorted, or searched by an identification number assigned by computer, by SSN (if maintained by the program), by facility, by business affiliation, by email address, or by the name of the individual, or other data fields previously identified in this SORN. Note that when DHS uses a third-party identity service provider for identity proofing, data elements collected by the third party on DHS's behalf are not retained by DHS unless specifically required by the program or application.

Safeguards:

Information in this system is safeguarded in accordance with applicable laws, rules and policies, including the DHS IT Security Program Handbook and DHS Information Security Program Policy and Handbook. DHS uses trusted identity service providers including those certified through the Trust Framework Adoption Process by Federal Identity Credential and Access Management (FICAM). The DHS/ALL-037 E-Authentication Records system of records security protocols also meet multiple NIST Security Standards from Authentication to Certification and Accreditation.

Records in the DHS/ALL-037 E-Authentication Records system of records will be maintained in a secure, password-protected, electronic system that uses security hardware and software including: Multiple firewalls, active intruder detection, and role-based access controls. Additional safeguards 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 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 NARA's General Records Schedule (GRS) 24, section 6, ``User Identification, Profiles, Authorizations, and Password Files.'' Inactive records are destroyed or deleted six years after the user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later.

In addition, in accordance with NIST SP-800-63-2, a record of the registration, history, and status of each token and credential (including revocation) is maintained by the credential service provider

(CSP) or its representative. The record retention period of data for Level 2 and 3 credentials is seven years and six months beyond the expiration or revocation (whichever is later). The minimum record retention period for Level 4 credential data is ten years and six months beyond the expiration or revocations of the credential.

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;

[[Page 46862]]

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, trusted third-party identity service providers (which may use commercial identity verification information not accessed or maintained by DHS to perform knowledge-based authentication), public source data, other government agencies, or information already in other DHS records systems.

Exemptions claimed for the system:
None.

Dated: July 31, 2014.
Karen L. Neuman,
Chief Privacy Officer, Department of Homeland Security.
[FR Doc. 2014-18703 Filed 8-8-14; 8:45 am]
BILLING CODE 9110-9B-P