[Federal Register Volume 76, Number 32 (Wednesday, February 16, 2011)]
[Notices]
[Pages 9034-9038]
From the Federal Register Online via the Government Publishing Office [www.gpo.gov]
[FR Doc No: 2011-3490]

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2011-0007]

Privacy Act of 1974; Department of Homeland Security United States Citizenship and Immigration Services--DHS/USCIS--013 E-Verify Self Check System of Records

AGENCY: Privacy Office, DHS.

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 Department of Homeland Security system of records titled, ``Department of Homeland Security/United States Citizenship and Immigration Services--SORN DHS/USCIS--013 E-Verify Self Check System of Records.'' The U.S. Citizenship and Immigration Services E-Verify Self Check is voluntary and available to any individual who wants to check his own work authorization status prior to employment and facilitate correction of potential errors in federal databases that provide inputs into the E-Verify process. When an individual uses E-Verify Self Check, he will be notified either that 1. his information matched the information contained in federal databases and he would be deemed work-authorized, or 2. his information was not matched to information contained in federal databases which would be considered a ``mismatch.'' If the information was a mismatch, he will be given instructions on where and how to correct his record(s). This newly established system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before March 18, 2011. This new system will be effective March 18, 2011.

ADDRESSES: You may submit comments, identified by docket number DHS-2011-0007 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: 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://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 please contact: Janice M. Jackson, Acting Privacy Branch Chief, Verification Division, U.S. Citizenship and Immigration Services, Department of Homeland Security, Washington, DC 20529. For privacy issues please contact: Mary Ellen Callahan (703-235-0780), Chief Privacy Officer, Privacy Office, 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) United States Citizenship and Immigration Services (USCIS) proposes to establish a new DHS system of records titled, ``DHS/USCIS--013 E-Verify Self Check System of Records.''

E-Verify was mandated by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Public Law (Pub. L.) 104-208, September 30, 1996. The E-Verify Program is a free and mostly voluntary DHS program implemented by the USCIS Verification Division and operated in collaboration with the Social Security Administration (SSA) to determine work authorization. It compares information provided by employees on the Employment Eligibility Verification, Form I-9, against information in SSA, DHS, and Department of State (DoS) databases in order to verify an employee's work authorization. Section 404(d) requires that the system be designed and operated to maximize the reliability and ease of use. Therefore, DHS has developed E-Verify Self Check.

USCIS developed E-Verify Self Check to enable an individual to check his work authorization status prior to employment and facilitate

correction of

[[Page 9035]]

potential errors in federal databases that provide inputs into the E-Verify process. Through the E-Verify Self Check secure web portal, an individual will be able to check his work authorization status by first providing information to authenticate his identity, and subsequently providing work authorization information based in part on information normally provided on Form I-9 employment documentation. Prior to E-Verify Self Check, only employers could verify work authorization for newly hired employees. With the introduction of E-Verify Self Check, upon successful identity authentication, an individual will be able to query E-Verify directly. If the information provided by the individual matches the information contained in federal databases (SSA, DHS, DoS) a result of ``work authorization confirmed'' is displayed to the individual. If the information was a mismatch, E-Verify Self Check will provide the individual a result of ``Possible mismatch with SSA'' or ``Possible mismatch with Immigration Information.'' E-Verify Self Check will also provide the individual instructions on how to request correction of these potential errors in records contained in these federal databases should the individual choose to do so prior to any formal, employer run E-Verify query process. In rare cases, an individual may still receive a potential mismatch during a normal E-Verify query because the record cannot be changed. The individual is not required to correct the record mismatches that were identified by E-Verify Self Check.

E-Verify Self Check Process Details

E-Verify Self Check involves a two-step process: (1) Identity authentication of the individual; and (2) an E-Verify query to confirm the individual's current work authorization status. The first step, identity authentication, utilizes a third party Identity Proofing (IdP) service to generate knowledge-based questions based on commercial identity verification information, collected by third party companies from financial institutions, public records, and other service providers. The information accessed by the IdP may include information, such as the individual's commercial transaction history, mortgage payments, or past addresses. An individual must correctly answer these knowledge-based questions generated by the IdP in order to authenticate his identity and enable him to use E-Verify Self Check. In order to generate these knowledge-based questions, the IdP service collects basic personally identifiable information (PII) from the individual including name, address of residence, date of birth, and optionally the individual's Social Security number (SSN). Each individual will be asked a minimum of two and a maximum of four knowledge-based questions. If there is not enough commercial identity verification information from financial institutions, public records, and other service providers to generate two questions, the individual's identity cannot be authenticated and he will not be able to continue through E-Verify Self Check. The fact that an individual was unable to use the IdP service will be sent to E-Verify, but no other information. The IdP will send a transaction number, the fact that knowledge based questions could not be generated and the date and time of the transaction, so that USCIS may keep a statistic of how many individuals are unable to use the IdP.

If there is sufficient information to generate two to four questions, the IdP will evaluate the answers to the questions and return a pass/fail indicator to USCIS. If the individual does not successfully answer the questions generated by the IdP, he will not be authenticated and he will not be able to continue through E-Verify Self Check. Neither the questions asked by the IdP service nor the answers provided by the individual are retained by the IdP. The IdP will send a transaction number, the reason for failure, the date and time of the transaction, and an error code to E-Verify, to facilitate troubleshooting and system management and improvement so that USCIS may keep statistics of how many individuals are unable to use the IdP and therefore Self Check. All PII entered by the individual during the IdP session and any questions that might have been generated by the IdP are deleted at the end of the session. Nothing is stored or retained in E-Verify Self Check. This information cannot be linked back to the individual.

If the individual is able to answer the questions; his identity is authenticated, a pass indicator is returned to E-Verify, and the individual will continue through E-Verify Self Check. E-Verify will receive a pass indication and the name, date of birth, and SSN (if provided) will be provided back to E-Verify. Residence address will not be passed to E-Verify.

When there are multiple attempts to authenticate an individual, which indicates possible fraud, the DHS contract authorizes the IdP to notify the provider of the information of potential fraud and to terminate access to E-Verify Self Check.

The Fair Credit Reporting Act (FCRA) requires the IdP to retain the fact of an inquiry. The IdP maintains the time/date stamp and inquiry type (credit check, identity check, etc.) so that the inquiry is noted in the individual's credit record and can be audited at a later date. The E-Verify Self Check inquiry is an identity check, and therefore will not affect an individual's credit score. These types of inquiries are not shown to third parties who may request copies of credit reports.

Under FCRA, an individual has the right to know who has reviewed

his credit report and the individual can place a fraud alert on his credit file. If an individual has placed a fraud alert on his credit file, the individual will not be able to authenticate for E-Verify Self Check purposes.

Upon identity authentication, the individual moves to step 2: an E-Verify query to identify current work authorization status. The IdP passes the name, date of birth and SSN (if provided). In order to ensure that the information belongs to the individual who originally passed the identity authentication step, these data elements cannot be altered. The individual will be required to enter additional information based on the documentation he would present to an employer for the Form I-9 process. The additional information collected from an individual depends on his citizenship status and the document chosen to present for work authorization. This could include: citizenship status; Alien Number (if non-citizen); passport number; Form I-94 number; and/or lawful permanent resident card or work authorization document (EAD) number. This represents the same information that is collected for the Form I-9 process and the basic E-Verify query.

E-Verify Self Check will query E-Verify through a web service connection and will present either an indication that an individual's information matched government records and that E-Verify would have found the individual work-authorized or that the information is a possible mismatch to government records. If the individual receives a ``possible mismatch with SSA/Immigration Information'' response, E-Verify Self Check will provide guidance on how to correct potential errors in the records. The individual will be asked whether they would like to resolve the mismatch or not. If the individual chooses not to resolve the mismatch, E-Verify will close the case. If the individual chooses to resolve the SSA mismatch, a form will be generated that contains the individual's first and last

[[Page 9036]]

name, the date and time of the E-Verify query, the E-Verify case number, and detailed instructions on how to resolve the mismatch. If the individual decides to resolve an Immigration Information mismatch, E-Verify Self Check provides instructions to contact E-Verify Customer Contact Office (CCO) to assist in the correction of immigration records 72 hours after the initial query to speak with a status verification representative. If the representative is unable to correct the record, the individual will be advised of actions necessary to correct the error.

The main benefit of E-Verify Self Check is to facilitate the identification and correction of potential errors in federal databases that provide inputs into the E-Verify system thereby improving the E-Verify process for both the employee and the employer. Prior to the introduction of E-Verify Self Check, an individual did not have the ability to identify potential issues associated with his work authorization status until after receiving adverse notification from employers. E-Verify Self Check provides a vehicle for an individual to proactively check work authorization status prior to the employer conducting the E-Verify inquiry.

There may be instances when an individual is unable to authenticate his identity using the IdP service. For example, the IdP may not be able to generate knowledge-based questions if sufficient data pertaining to him cannot be located or if he has placed a lock or alert on his information. In addition, an individual may not receive a passing score because the IdP information maintained is incorrect. If someone is unable to authenticate through the IdP but still wants to determine work authorization status prior to hire, USCIS will provide information on how to visit an SSA field office, access Social Security yearly statements, call USCIS, or submit a Freedom of Information Act/Privacy Act request to access work authorization records. The individual will also be advised to check the information at the various credit bureaus and through a free credit check site.

This newly established system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which the U.S. 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 U.S. 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.

Below is the description of the DHS/USCIS--013 E-Verify Self Check 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/USCIS--013 E-Verify Self Check.

System name:
DHS/USCIS--013 E-Verify Self Check.

Security classification:
Unclassified, sensitive.

System location:
Records are maintained at the USCIS Headquarters in Washington, D.C. and field offices.

Categories of individuals covered by the system:
Individuals seeking to check employment eligibility under the Immigration and Naturalization Act (INA). This includes U.S. citizens as well as non-U.S. citizens.

Categories of records in the system:
E-Verify Self Check is a two-step process: (1) identity authentication and (2) confirmation of work authorization status. The first step of the process is the identity authentication. E-Verify Self Check will use a third party commercial identity assurance service provider (IdP) using commercial identity verification information, collected by third-party companies from financial institutions, public records, and other service providers to verify an individual's identity. The IdP will collect information about the individual who has elected to use E-Verify Self Check.
The IdP will collect the following information from all individuals in order to generate the questions:
Name (last, first, middle initial, and maiden);
Date of birth;
Address of Residence; and
SSN(if provided).
The questions asked by the IdP and the answers provided by the individual are not provided to USCIS. If an individual fails the identity authentication portion of E-Verify Self Check and therefore is unable to proceed to an actual query in E-Verify, none of the information listed above is provided to or retained by E-Verify Self Check. Only the transaction number, the reason for failure, the date and time of the transaction, and error code are retained by the IdP to facilitate troubleshooting and system management.
In the individual passes identity authentication, he will be redirected to the DHS/USCIS E-Verify Self Check screen to begin the E-Verify Self Check. The individual's name, date of birth, and SSN (if provided) that were entered during identity authentication is automatically pre-populated in E-Verify Self Check (E-Verify will not receive the address of residence). This information will be unchangeable to ensure that the information represents the individual whose identity has been authenticated. To begin the E-Verify Self Check process, the individual will be asked for additional information. This information will be based the on individual's citizenship status and the document chosen to prove work authorization. Documents chosen could include:
SSN (if not previously provided);
Document(s) type, associated number, and associated expiration date that demonstrates work authorization. These may include U.S. Passport, employment authorization document, I-495 Lawful Permanent resident card, or other documents and associated numbers as listed as acceptable Form I-9 verification documents.
This process is the same process as the basic E-Verify query and is described in the E-Verify PIA, dated May 4, 2010, and System of Records Notice dated May 19, 2010, 75 FR 28035.

Authority for maintenance of the system:
The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Public Law 104-208, dated September 30, 1996.

Purpose(s):
An individual will use E-Verify Self Check to determine work authorization status. E-Verify Self Check contracts with an IdP in order to provide identity authentication.

[[Page 9037]]

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 (DOJ), including U.S. 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 U.S. 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 request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) 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. 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) 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 the E-Verify Program, which includes possible fraud, discrimination, or employment based identity theft and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To an individual utilizing E-Verify Self Check in order to determine his own work authorization in the United States.

I. To a third party commercial identity assurance provider (IdP) under contract with the Department, but only the name, date of birth, address of residence, and Social Security number (if provided), for the purposes of authenticating an individual who is seeking to access the USCIS E-Verify Self Check for employment eligibility.

When there are multiple attempts to authenticate an individual, which indicates possible fraud, the DHS contract authorizes the IdP to notify the provider of the information of potential fraud and to terminate access to E-Verify Self Check. The IdP will share the fact of the inquiry with the appropriate credit bureau and monitor for potential fraudulent access in accordance with the Fair Credit Reporting Act (FCRA).

Disclosure to consumer reporting agencies:

DHS is using the services of a third party IdP to authenticate an individual's identity. The third party IdP uses commercial identity verification information which is collected by third party companies from financial institutions, public records, and other service providers to create the knowledge-based questions used to authenticate identity. This information does not belong to DHS nor will information from other sources relied upon by the third party provider be collected and/or retained by DHS. FCRA requires the IdP to retain the fact of an inquiry. The IdP will maintain time/date stamp and inquiry type (credit check, identity check, etc.) so that the inquiry is noted in the individual's credit record and can be audited at a later date. The E-Verify Self Check inquiry is an identity check, and therefore will not affect an individual's credit score. These types of inquiries are not shown to third parties who may request copies of credit reports. Under FCRA, an individual has the right to know who has reviewed his credit report and the individual can place a fraud alert on his credit file. If an individual has placed a fraud alert on his credit file, the individual will not be able to authenticate for E-Verify Self Check purposes.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records in this system are stored electronically, on magnetic disc, tape, digital media, and CD-ROM. All personal information entered by the individual as part of the IdP process and any questions that might have been generated by the third party data IdP are deleted at the end of the session. Nothing is stored or retained in E-Verify Self Check. Only the transaction number, the reason for failure, the date and time of the transaction, and error code are retained to facilitate troubleshooting and system management. Because the IdP accesses an individual's credit history to perform the authentication, it will retain audits of the individual's E-Verify Self Check inquiry to comply with legal obligations, specifically, the FCRA. The FCRA requires that an inquiry be noted in the individual's credit record.

Retrievability:
Records related to the IdP portion of the program can be retrieved by the following fields:
E-Verify Self Check unique transaction ID;
IdP Unique Transaction ID;
E-Verify Self Check transaction time/date stamp;
Failure of the IDP transaction; and
Reason for Failure (i.e., could not generate questions/ answered incorrectly/system error)
For the actual E-Verify Self Check query, the information will be retrieved

[[Page 9038]]

by name, Alien Number, I-94 Number, Receipt Number, Passport (U.S. or Foreign) Number, or Social Security number of the individual as discussed in the E-Verify SORN dated May 19, 2010.

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 the 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:
The retention schedule is currently under development with the National Archives and Records Administration (NARA). The proposed retention schedule for the query and response to the query is for one (1) year in order to allow time for management analysis and proper reporting.

System Manager and address:
Chief, Verification Division, U.S. Citizenship and Immigration Services, Washington, DC 20529.

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 USCIS 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, 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 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:
See ``Notification procedure'' above.

Contesting record procedures:
See ``Notification procedure'' above.

Record source categories:
Records are obtained from several sources including: (A) Information collected from individuals requesting their work authorization status; (B) information collected from federal databases for work authorization, (C) information created by E-Verify, including its monitoring and compliance activities; and (D) pass notification from the IdP when an individual has successfully completed identity authentication.

Exemptions claimed for the system:
None.

Dated: February 10, 2011.
Mary Ellen Callahan,
Chief Privacy Officer, Department of Homeland Security.
[FR Doc. 2011-3490 Filed 2-15-11; 8:45 am]
BILLING CODE 9117-97-P