Billing Code: 3410-ZV

UNITED STATES DEPARTMENT OF AGRICULTURE

Office of the Secretary

Privacy Act of 1974; Revised System of Records

AGENCY: Office of the Chief Information Officer, USDA

ACTION: Notice of the revision of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Agriculture proposes to revise an existing Department of Agriculture system of records notice now titled, USDA/OCIO-2 eAuthentication Service (eAuth). The USDA eAuth provides the public and government businesses with a single sign-on capability for USDA applications, management of user credentials, and verification of identity, authorization, and electronic signatures. USDA's eAuth collects customer information through an electronic self-registration process provided through the eAuth Web site. This System of Records Notice was previously published as "USDA eAuthentication Service" in Federal Register Vol. 77, No. 50 on Wednesday, March 14, 2012. The revision reflects updates to the system name; the system location; routine uses; storage policies; safeguards; retention and disposal; identity proofing individuals, the system manager; and notification, record access, and contesting procedures.

DATES: Submit comments on or before *[INSERT DATE 40 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]*. This new system will be effective *[INSERT DATE 40 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]*.

ADDRESSES: You may submit comments, identified by docket number USDA/OCIO-2 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: (970) 295-5238
- Mail: Adam Zeimet, Branch Chief, Identity Access Branch, eAuthentication, 2150 Centre Avenue, Building A, Suite 350, Fort Collins, Colorado 80526
- 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:

Adam Zeimet, Program Manager, (970) 295-5678, 2150 Centre Avenue, Building A, Suite 350, Fort Collins, Colorado 80526. For privacy issues, please contact: Kelvin Fairfax, Chief Privacy Officer, Technology Planning, Architecture and E-Government, Office of the Chief Information Officer, Department of Agriculture, Washington, D.C. 20250.

SUPPLEMENTARY INFORMATION:

I. Background

The USDA eAuthentication Service provides USDA Agency customers and employee's single sign-on capability and electronic authentication and authorization for USDA Web applications and services. Through an online self-registration process, USDA Agency customers and employees can obtain accounts as authorized users that will provide access to USDA resources without needing to re-authenticate within the context of a single Internet session. Once an account is activated, users may use the associated user ID and password that they created to access USDA resources that are protected by eAuthentication. Information stored in the eAuthentication Service may be shared with other USDA components, as well as appropriate Federal, State, local, tribal, foreign, or international government agencies as outlined in the routine uses or authorized by statute. This sharing will take place only after USDA determines that the receiving component or agency has a need to know the information to carry out agency mission, national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice. The revisions to this system of records include: updating the system location, storage policies, storage safeguards, retention and disposal policies; the system manager's location; the practice of identity proofing individuals; record retrieval; and the notification, record access, & contesting procedures in order to be consistent with the Department's best practices.

In addition, the routine uses were amended as follows:

- Routine Use 1. is modified adding account management and user profile management
- Routine Use 8. is added to permit another federal agency or federal entity to investigate breaches and remedy risk to individuals

- Routine Use 9. is added for disclosure to credit bureaus to conduct identity proofing
- Routine Use 10. is added for disclosure for contractors to assist in administering the program
- Routine Use 11. Is added for disclosure of records to other federal agencies

Dated: __ January 18, 2017 _____

_____

Michael T. Scuse

Acting Secretary of Agriculture

System of Records

USDA/OCIO-2

System Name:

USDA/OCIO-2 eAuthentication Service

Security Classification:

Unclassified

System Location:
USDA- National Information Technology Center (NITC), 8930 Ward Pkwy, Kansas City, MO 64114
USDA- St. Louis Enterprise Data Center, 4300 Goodfellow Boulevard, St. Louis, MO 63120 US

Categories of Individuals Covered by the System:
This system contains records on individuals who applied for and were granted access to USDA applications and services that are protected by eAuthentication. This includes but not limited to public citizens, federal employees, contractor employees, affiliates, etc.

Categories of Records in the System:
The eAuthentication system will collect the information including but not limited to name, address, country of residence, telephone, email address, date of birth, user name, password, SSN (Capture Temporarily), challenge question, and challenge answer. The latter two types of information are used to validate a customer's identity for password reset. The system will request social security number for online identity proofing services through a verification process implemented with a credit bureau.

Authority for Maintenance on the System:
Government Paperwork Elimination Act (GPEA, Pub. L. 105-277) of 1998; Freedom to E-File Act (Pub. L. 106-222) of 2000; Electronic Signatures in Global and National Commerce Act (E-SIGN, Pub. L. 106-229) of 2000; eGovernment Act of 2002 (H.R. 2458/Pub L. 107-347); GRAMM–LEACH–BLILEY ACT (Pub L. 106-102).

Purpose(s):
The records in this system are used to electronically authenticate and authorize users accessing protected USDA applications and services. eAuthentication shares the user information with authorized federal agencies or contractor systems supporting a federal agency mission for centralized account management and user profile management for USDA.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of Such Uses. Records in this system may be disclosed as follows:

1. To external Web applications or information technology systems integrated with the government's federated architecture for authentication, identity management, and user profile management for USDA. Prior to any disclosure of information under this architecture, the user will request access to an external application with their USDA credential. All external applications will have

undergone rigorous testing before joining the architecture. The eAuthentication Service acts as a single sign-on point for USDA Agency applications, allowing a USDA customer to sign onto any USDA applications for which they have been authorized.

2. When a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program, statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate agency, whether Federal, foreign, State, local, tribal, or other public authority responsible for enforcing, investigating, or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative, or prosecutive responsibility of the receiving entity. Referral to the appropriate agency, whether Federal, State, local, or foreign, charged with the responsibility of investigating or prosecuting violation of law, or of enforcing or implementing a statute, rule, regulation, or order issued pursuant thereto, of any record within this system when information available indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature.

3. To a court or adjudicative body in a proceeding when: (a) USDA or any component thereof; or (b) any employee of USDA in his or her official capacity; or (c) any employee of USDA in his or her individual capacity where USDA has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, USDA determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by USDA to be for a purpose that is compatible with the purpose for which USDA collected the records.

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

5. Disclosure at the individuals' request to any Federal department, State, local agencies, or USDA partners including but not limited to contractor systems supporting the government mission utilizing or interfacing with eAuthentication to provide electronic authentication. The disclosure of this information is required to securely provide, monitor, and analyze the requested program, service, registration, or other transaction.

6. To the Department of Justice when: (a) USDA or any component thereof; or (b) any employee of USDA in his or her official capacity where the Department of Justice has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, USDA determines that the records are both relevant and necessary to the litigation and the use of such records by the Department of Justice is therefore deemed by USDA to be for a purpose that is compatible with the purpose for which USDA collected the records.

7. To appropriate agencies, entities, and persons when (1) USDA suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) USDA has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, USDA (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with USDA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

8. To another Federal agency or Federal entity, when information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the agency

(including its information systems, programs and operations), the Federal Government, or national security.

9. Disclosure to credit bureaus to conduct online identity proofing of users including but not limited to public citizens, federal employees, contractor employees, affiliates, etc., for the purpose of remotely verifying the users identity in using eAuthentication account management practices (e.g. Issuing an account & credential, and account recovery).

10. Contract Disclosure. If the Department contracts with an entity for the purpose of performing any function that requires disclosure of records including but not limited to helpdesk operations, password resets, system administration, application operations, program support. The Department may disclose the records as a routine use to those contract employees. Before entering into such a contract, the Department shall require the contractor to maintain Privacy Act safeguards as required under 5 U.S.C. 552a(m) with respect to the records in the system.

11. Disclosure may be made to a private contractor or Federal agency for the purpose of collating, analyzing, aggregating or otherwise refining records for official business in this system. The contractor or Federal agency will be required to maintain Privacy Act safeguards with respect to these records.

Policies/Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System

Storage:
Records are stored and maintained electronically on USDA owned and operated systems in Kansas City, MO and St. Louis, Missouri.

Retrievability:
Records can be retrieved by a search of user profile attributes including but not limited to Personal Identity Verification (HSPD-12 PID) card identifiers, UserName (Login ID), Last Name, First Name, Email, system ID (eAuth Internal ID), challenge question, and challenge answer. The latter two types of information are used to validate a customer's identity for helpdesk services only those individuals with approved access rights have this authority and data accessibility. USDA staff and contractors (acting as authorized agents) access information that is necessary to fulfill customer requests, provide end-user technical support and to operate and administer the system.

Safeguards:
Records are accessible only to authorized personnel. Protection of the records is ensured by appropriate technical controls. The physical security of the system is provided by restricted building access. In addition, increased security is provided by encryption of data when transmitted. SSN is masked during the capture process when a user enters on the web form. The system has undergone an Assessment and Authorization (A&A) by the OCIO Designated Approving Authority via Agricultural Security Operations Center (ASOC).

Retention and Disposal:
Records in this system will be retained in accordance with approved retention schedules, including: (31) General Retention Schedule (DAA-GRS-2013-0006-0004), which provides for annual cut-off and for destruction 6 years after cutoff or longer if required for business use; (61)

General Retention Schedule (N1-GRS-07-3, item 13a2), which provides for annual cut-off and for destruction 7 years and 6 months to 20 years to 6 months after cut-off; and additional approved schedules may apply. Destruction of records shall occur in the manner(s) appropriate to the type of record, such as but not limited to shredding of paper records and/or deletion of computer records in accordance with federal requirements.

System Manager and Address:
Program Manager - Identity and Access Management, 2150 Centre Avenue, Fort Collins, CO 80526

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.da.usda.gov/foia.htm 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 FOIA Officer, Department of Agriculture, 1400 Independence Avenue, S.W., Washington, D.C. 20250.
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 FOIA Officer, Department of Agriculture, 1400 Independence Avenue, S.W., Washington, D.C. 20250.
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 USDA component agency may have responsive records,
• If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.
Without this bulleted information the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

Record Access Procedures:
See "Notification procedure" above.

Contesting Record Procedures:
Any individual may contest information contained within a record in the system that pertains to him/her by submitting a written request to the system manager at the address above. Include the reason for contesting the record and the proposed amendment to the information with supporting documentation to show how the record is inaccurate.

Record Source Categories:

Information maintained in the system will be submitted but not limited to public citizens, federal employees, contractor employees, affiliates, etc.. When a user wishes to transact with USDA or its partner organizations electronically, the user must enter name, address, country of residence, telephone, date of birth, username, and password. To elevate the user to conduct official business with USDA the user must be identity proofed requiring social security number being queried through a national credit bureau. As the USDA eAuthentication Service is integrated with other government or private sector authentication systems, data may be obtained from those systems to facilitate single-sign on capabilities with the user's permission.

Exemptions Claimed for this System:
None.

U.S. DEPARTMENT OF AGRICULTURE NARRATIVE STATEMENT ON REVISED EAUTHENTICATION SYSTEM OF RECORDS UNDER THE PRIVACY ACT OF 1974 USDA/OCIO-2 EAUTHENTICATION SERVICE

The U.S. Department of Agriculture (USDA) eAuthentication Service provides USDA Agency customers and employees single sign-on capability and electronic authentication and authorization for USDA Web applications and services. Through an online self-registration process, USDA Agency customers and employees can obtain accounts as authorized users that will provide access to USDA resources without needing to re-authenticate within the context of a single Internet session. Once an account is activated, users may use the associated user ID and password that they created to access USDA resources that are protected by eAuthentication. Information stored in the eAuthentication Service may be shared with other USDA components, as well as appropriate Federal, State, local, tribal, foreign, or international government agencies as outlined in the routine uses or authorized by statute. This sharing will take place only after USDA determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice. USDA is publishing the routine uses pursuant to which it may disclose information about individuals to the extent the disclosure is consistent with the purpose for which the information was collected. Routine uses include disclosure to external Web applications upon user request, to other government agencies for law enforcement purposes if the record on its face or in conjunction with other records indicates a violation of law, to a court or adjudicative body if relevant and necessary to appropriate litigation, to a congressional office upon written request of the individual, to other government entities of USDA partners upon user request, to USDA contractors or industry to identify fraud, waste, or abuse to the Department of Justice if relevant and necessary for appropriate litigation, or to agencies, entities, or persons to prevent or remedy security breach. The authority for maintaining this system is derived from: Government Paperwork Elimination Act (GPEA, Pub. L. 105-277) of 1998; Freedom to E-File Act (Pub. L. 106-222) of 2000; Electronic Signatures in Global and National Commerce Act (E-SIGN, Pub. L. 106-229) of 2000; eGovernment Act of 2002 (H.R. 2458).

Probable or potential effects on the privacy of individuals:

Although there is some risk to the privacy of individuals, that risk is outweighed by the benefits to those individuals who will be able to access multiple programs and applications with a single login. In addition, the safeguards in place will protect against unauthorized disclosure. Records are accessible only to individuals who are authorized, and physical and electronic safeguards are employed to ensure security. eAuthentication has a current Authority to Operate obtained via the completion Certification and Accreditation based on the Risk Management Framework. A satisfactory risk assessment has been performed.

OMB information collection requirements:

OMB information collection approval: OMB No. 0503-0014

[FR Doc. 2017-01767 Filed: 1/25/2017 8:45 am; Publication Date: 1/26/2017]