Notices

Federal Register
Vol. 71, No. 143
Wednesday, July 26, 2006

This section of the FEDERAL REGISTER contains documents other than rules or proposed rules that are applicable to the public. Notices of hearings and investigations, committee meetings, agency decisions and rulings, delegations of authority, filing of petitions and applications and agency statements of organization and functions are examples of documents appearing in this section.

DEPARTMENT OF AGRICULTURE

Privacy Act of 1974: Report of a New System of Records

AGENCY: Office of the Chief Information Officer, USDA.

ACTION: Notice of proposed new system of records; request for comments.

SUMMARY: Notice is hereby given that the United States Department of Agriculture (USDA) proposed to create a new Privacy Act system of records, entitled ''USDA eAuthentication Service.'' The system is owned, administered, and secured by the Office of the Chief Information Officer (OCIO), a USDA staff office. The primary purpose of the eAuthentication Service is to provide verification of customer identity, authorization, and electronic signatures for USDA application and service transactions.

DATES: *Effective Date:* This notice will be adopted without further publication on August 25, 2006, unless modified by a subsequent notice to incorporate comments received from the public. USDA invites comments on all portions of this notice. Comments must be received by the contact listed on or before August 25, 2006.

FOR FURTHER INFORMATION CONTACT: Owen Unangst, Program Manager, Office of the Chief Information Officer, United States Department of Agriculture, NRCS Information Technology Center, 2150 Centre Avenue Building A, Fort Collins, CO 80526–1891 or via e-mail at *owen.unangst@ftc.usda.gov.*

SUPPLEMENTARY INFORMATION: The Privacy Act (5 U.S.C. 552a(e)(4) requires the Department to publish in the **Federal Register** this notice or new or revised system of records managed by the Department. Pursuant to the Government Paperwork Elimination Act (GPEA, Pub. L. 105–277), the Freedom to E-File Act (Pub. L. 106–222), the Electronic Signature in Global and National Commerce Act (E–SIGN, Pub. L. 102–229), and the eGovernment Act of 2002 (H.R. 2458), USDA is creating a new system of records entitled ''USDA eAuthentication Service'' to be managed by the USDA Office of the Chief Information Officer (OCIO).

GPEA requires that Federal agencies provide citizens with secure electronic options for forms, filing, and other transactions needed to conduct official business with the government. The eAuthentication Service provides a trusted and secure infrastructure, which is primary to the delivery of eGovernment services in a GPEA compliant manner. eAuthentication support citizens' capabilities to conduct transactions with USDA by providing single sign-on capability to access USDA applications and services via the Internet, management of user credential, and verifications of identity, authorization, and electronic signature with USDA, its agencies, and partners. Benefits to citizens and USDA include a secure, consistent method of electronic authentication, a reduction in the cost to maintain redundant registration information, and reduced authentication system development and acquisition costs.

USDA eAuthentication collects information from citizens in order to provide accounts that facilitate the electronic authentication and authorization. The credentials and permissions associated with an account are what authenticates and authorizes a user to access a requested USDA resource. USDA obtains customer information through an electronic self-registration process provided through the eAuthentication Web site. The collected information will be secured in two ways: Appropriate technical security will be in place both during storage and transit; the physical security of the system will be provided by the hosting facility which restricts access to authorized personnel.

USDA customers can self-register for a Level 1 or Level 2 Access account. A Level 1 Access account provides users with limited access to USDA Web site portals and applications that have minimal security requirements. A Level 2 Access account enables users to conflict official electronic business transactions via the Internet, enter into a contract with USDA, and submit information electronically via the Internet to USDA Agencies. Due to the increased customer access associated with a Level 2 Access account, customers must be authenticated in person at a USDA Office by a local registration authority, in addition to an electronic self-registration. Once an account is activated, customers may use the associated user ID and password that they created to access USDA resources that are protected by the eAuthentication Service.

System of Records

SYSTEM NAME:

USDA eAuthentication Service.

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

USDA–NRCS Information Technology Center, 2150 Centre Avenue Building A, Fort Collins, CO 80526–1891; USDA-Rural Development, 1520 Market Street, St. Louis, MO 63103.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

This system contains records and related correspondence on individuals who can access USDA application and services that are protected by eAuthentication. This includes members of the public and USDA employees.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

This system contains records and related correspondence on individuals who can access USDA applications and services that are protected by eAuthentication. This includes members of the public and USDA employees.

CATEGORIES OF RECORDS IN THE SYSTEM:

The eAuthentication system will collect the following information from individuals when transacting electronically with USDA: name, address, country of residence, telephone, e-mail address, date of birth, and mother's maiden name. The system will also require users to create a user ID and password.

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).

PURPOSE(S):

The records in this system are used to electronically authenticate and authorize users accessing protected USDA applications and services.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

1. Disclosure to USDA applications protected by eAuthentication, as a user requests access to individual applications.

2. Disclosure to external Web applications integrated with the government's federated architecture for authentication. Under this architecture, the user will request access to an external application with their USDA credential prior to any disclosure of information. All external applications will have undergone rigorous testing before joining the architecture.

3. 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.

4. Disclosure to a court, magistrate, or administrative tribunal, or to opposing counsel in a proceeding before a court, magistrate, or administrative tribunal, of any record within the system that constitutes evidence in that proceeding, or which is sought in the course of discovery, to the extent that USDA determines that the records sought are relevant to the proceeding.

5. Disclosure to a congressional office from the record of an individual in response to any inquiry from the congressional office made at the request of that individual.

6. Disclosure at the individual's request to any Federal department, State or local agency, or USDA partner utilizing or interfacing with eAuthentication to provide electronic authentication for electronic transactions. The disclosure of this information is required to securely provide, monitor, and analyze the requested program, service, registration, or other transaction.

7. Disclosure to USDA employees or contractors, partner agency employees or contractors, or private industry employed to identify patterns, trends, and anomalies indicative of fraud, waste, or abuse.

8. Disclosure to determine compliance with program requirements.

POLICIES AND 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 St. Louis, MO, and Ft. Collins, CO.

RETRIEVABLY:

Records can be retrieved by name, username, or system ID.

SAFEGUARD:

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. The system has undergone a Certification and Accreditation.

RETENTION AND DISPOSAL:

Since records are maintained electronically, they will be retained indefinitely.

SYSTEM MANAGER(S) AND ADDRESS:

Owen Unangst, NRCS Information Technology Center, 2150 Centre Avenue Building A, Fort Collins, CO 80526–1891.

NOTIFICATION PROCEDURE:

An individual may request information regarding this system of records or information as to whether the system contains records pertaining to such individual from the Fort Collins office. The request for information should contain the individual's name, username, address, and email address. Before information of any record is released, the system manager may require the individual to provide proof of identify or require the requester to furnish authorization from the individual to permit release of information.

RECORD ACCESS PROCEDURES:

An individual may obtain information as to the procedures for gaining access to a record in the system, which pertains to such individual, by submitting a request to the Privacy Act Officer, 1400 Independence Avenue, SW., South Building, Washington, DC 20250–3700. The envelope and letters should be marked ''Privacy Act Request.'' A request for information should contain name, address, username, name of system of records, year of records in question, and any other pertinent information to help identify the file.

CONTESTING RECORD PROCEDURES:

Procedures for contesting records are the same as procedures for record access. 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 from the system will be submitted by the user. 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, mother's maiden name, username, and password. 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.

EXEMPTIONS CLAIMED FOR THIS SYSTEM:

None.

Dated: July 12, 2006.

Mike Johanns,

Secretary.

Privacy Act System USDA/OCIO–2 Narrative Statement

The purpose of this system of records for the eAuthentication Service is to identify how the user information collected is protected, used, and verified. Through a self-registration process USDA customers and employees are able to obtain accounts as authorized users that will enable them to access USDA Web applications and services. Additionally, users of the eAuthentication system are able to securely and confidently conduct business transactions with the USDA electronically via the Internet.

The information collected will be used to create eAuthentication accounts that are used to authenticate users to USDA Web applications. In addition, customer and employee account information is provided to USDA applications that the user chooses to access, in order to facilitate authorization and business transactions.

The authority for maintaining this system of records lies within the Government Paperwork Elimination Action (Sections 1702, 1703, 1705), the Freedom to E-File Act (Section 3 [7 U.S.C. 7032], Section 5 [7 U.S.C. 7034], and Section 6 [7 U.S.C. 7035], the Electronic Signatures in Global and National Commerce Act [15 U.S. 7001],

and the E-Government Act (Title III: FISMA of 2002 Section 301).

Within USDA, access to system data is granted on a limited basis to USDA customers, employees, administrators, help desk individuals, and other Federal agencies to facilitate electronic user authentication and authorization. Users can use their account's user ID and password to access to modify basic personal data such as address and email. Users do not have access to modify sensitive data such as level of access of permissions associated with an account. Only system administrators have access to update sensitive fields, and only do so when a ticket is escalated from the help desk.

System administrators have access to user information on a limited basis allowing them to only perform their specific job function. Access is limited to administrators on a least privileged basis utilizing separation of duties. Administrators and help desk persons have eAuthentication accounts with the appropriate level of access and permissions that allow them to access and modify user data. These permissions are granted by a limited number of management personnel.

Information obtained by the eAuthentication Service is stored and maintained electronically on secure USDA-owned and operated systems in St. Louis, MO and Fort Collins, CO. In addition, information stored electronically will be available only to authorized personnel, whose identity will be authenticated by eAuthentication Service.

The system provides for eight types of routine user releases, as follows:

Routine use 1 permits disclosure to USDA applications protected by eAuthentication, as a user requests access to individual applications.

Routine use 2 permits disclosure to external Web applications integrated with the government's federated architecture for authentication. Under this architecture, the user will request access to an external application with their USDA credential prior to any disclosure of information. All external applications will have undergone rigorous testing before joining the architecture.

Routine use 3 permits 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.

Routine use 4 permits disclosure to a court, magistrate, or administrative tribunal, or to opposing counsel in a proceeding before a court, magistrate, or administrative tribunal, of any record within the system that constitutes evidence in that proceeding, or which is sought in the course of discovery, to the extent that USDA determines that the records sought are relevant to the proceeding.

Routine use 5 permits disclosure to a congressional office from the record of an individual response to any inquiry from the congressional office made at the request of that individual.

Routine use 6 permits disclosure at the individuals' request to any Federal department, State or local agency, or USDA partner utilizing or interfacing with eAuthentication to provide electronic authentication for electronic transactions. The disclosure of this information is required to securely provide, monitor, and analyze the requested program, service, registration, or other transaction.

Routine use 7 permits disclosure to USDA employees or contractors, partner agency employees or contractors, or private industry employed to identify patterns, trends, and anomalies indicative of fraud, waste, or abuse.

Routine use 8 permits disclosure to determine compliance with program requirements.

A copy of the forms developed to collection information is attached to this report. These proposed information collections are at OMB for review and clearance in conjunction with the Paperwork Reduction Act.

The system of records will not be exempt from any provisions of the Privacy Act.

eAuthentication Forms for Collection for SORN Narrative Statement

Main Page: *http://www.eauth.egov.usda.gov/index.html.*

Select *Create an Account* from *Left Navigation Bar*. From the first sentence on this page, select the *USDA Employee Create an Account* link. Select the ''Continue'' button at the bottom right of the screen to move through the account creation process. Select the ''Continue'' button at the bottom right of the screen again, which opens the *Employee Account Creation, Step 1 of 6: Employee Information* page. Follows steps.

[FR Doc. 06–6396 Filed 7–25–06; 8:45 am]

BILLING CODE 3410–15–M

DEPARTMENT OF AGRICULTURE

Animal and Plant Health Inspection Service

[Docket No. APHIS–2006–0015]

Availability of an Addendum to Environmental Assessment and Finding of No Significant Impact for Field Release of Genetically Engineered Pink Bollworm

AGENCY: Animal and Plant Health Inspection Service, USDA.

ACTION: Notice.

SUMMARY: We are advising the public that we have supplemented with an addendum the environmental assessment for a proposed field trial of pink bollworm genetically engineered to express green fluorescence as a marker. The Animal and Plant Health Inspection Service (APHIS) proposes to use this marked strain to assess the effectiveness of lower doses of radiation to create sterile insects for its pink bollworm sterile insect program. This program, using sterile insect technique, has been conducted by APHIS, with State and grower cooperation, since 1968. Data gained from this field experiment will be used to improve the current program. APHIS has supplemented its environmental assessment in order to evaluate a new location and new conditions for the field test and has concluded that this field test will not have a significant impact on the quality of the human environment. Based on its finding of no significant impact, APHIS has determined that an environmental impact statement need not be prepared for this field test.

DATES: *Effective Date:* July 26, 2006.

ADDRESSES: You may read the environmental assessment (EA), the supplement, the finding of no significant impact (FONSI), and any comments that we received on Docket No. APHIS–2006–0015 in our reading room. The reading room is located in room 1141 of the USDA South Building, 14th Street and Independence Avenue, SW., Washington, DC. Normal reading room hours are 8 a.m. to 4:30 p.m., Monday through Friday, except holidays. To be sure someone is there to help you, please call (202) 690–2817 before coming. The supplemented EA and FONSI are also available on the Internet at *http://www.aphis.usda.gov/brs/aphisdocs/05_09801r_ea.pdf.*

FOR FURTHER INFORMATION CONTACT: Dr. Robyn Rose, Biotechnology Regulatory Services, APHIS, 4700 River Road Unit 147, Riverdale, MD 20737–1236; (301) 734–0489. To obtain copies of the EA,