

Notices

Federal Register

Vol. 91, No. 169

Wednesday, September 2, 2026

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

Economic Research Service

Agency Information Collection Activities: Comment Request

AGENCY: Economic Research Service, U.S. Department of Agriculture (USDA).

ACTION: Notice and request for comments.

SUMMARY: In accordance with the Paperwork Reduction Act of 1995, this notice announces the intention of the Economic Research Service (ERS) to request an extension of a currently approved information collection titled "Data Security Requirements for Accessing Confidential Data." ERS plans to collect information from the public to fulfill its data security requirements when providing access to restricted use data for the purpose of evidence building. ERS's data security agreements and other paperwork along with the corresponding security protocols allow ERS to maintain careful controls on confidentiality and privacy, as required by law.

DATES: Written comments on this notice must be received by November 2, 2026 to be assured of consideration.

ADDRESSES: Address all comments concerning this notice to ers.pra@usda.gov identified by docket number 0536-0079.

FOR FURTHER INFORMATION CONTACT: Requests for additional information or copies of this information collection should be directed to ers.pra@usda.gov.

SUPPLEMENTARY INFORMATION:

Title of Collection: Data Security Requirements for Accessing Confidential Data.

OMB Control Number: 0536-0079.

Expiration Date of Current Approval: March 31, 2027.

Type of Request: Intent to extend a currently approved information collection for 3 years.

Abstract: Title III of the Foundations for Evidence-Based Policymaking Act of 2018 (hereafter referred to as the Evidence Act) mandates that OMB establish a Standard Application Process (SAP) for requesting access to certain confidential data assets. Specifically, the Evidence Act requires OMB to establish a common application process through which agencies, the Congressional Budget Office, State, local, and Tribal governments, researchers, and other individuals, as appropriate, may apply for access to confidential data assets collected, accessed, or acquired by a statistical agency or unit. This new process will be implemented while maintaining stringent controls to protect confidentiality and privacy, as required by law.

Data collected, accessed, or acquired by statistical agencies and units is vital for developing evidence on conditions, characteristics, and behaviors of the public and on the operations and outcomes of public programs and policies. This evidence can benefit the stakeholders in the programs, the broader public, as well as policymakers and program managers at the local, State, Tribal, and National levels. The many benefits of access to data for evidence building notwithstanding, ERS is required by law to maintain careful controls that allow it to minimize disclosure risk while protecting confidentiality and privacy.

The fulfillment of ERS's data security requirements places a degree of burden on the public, which is outlined below.

The SAP Portal is a web-based application for the public to request access to confidential data assets from federal statistical agencies and units. The objective of the SAP Portal is to increase public access to confidential data for the purposes of evidence building and reduce the burden of applying for confidential data. Once an individual's application in the SAP Portal has received a positive determination, the data-owning agency(ies) or unit(s) will begin the process of collecting information to fulfill their data security requirements.

The paragraphs below outline the SAP Policy, the steps to complete an application through the SAP Portal, and the process for agencies to collect information fulfilling their data security requirements.

The SAP Policy

At the recommendation of the ICSP, the SAP Policy establishes the SAP to be implemented by statistical agencies and units and incorporates directives from the Evidence Act. The policy is intended to provide guidance as to the application and review processes using the SAP Portal, setting forth clear standards that enable statistical agencies and units to implement a common application form and a uniform review process. The SAP Policy renewal was submitted to the public for comment in June 2025 (90 FR 25380). The renewal policy was approved and has a current expiration date of 12-31-2028.

The SAP Portal

The SAP Portal is an application interface connecting applicants seeking data with a catalog of data assets owned by the federal statistical agencies and units. The SAP Portal is not a new data repository or warehouse; confidential data assets will continue to be stored in secure data access facilities owned and hosted by the federal statistical agencies and units. The SAP Portal will provide a streamlined application process across agencies, reducing redundancies in the application process. This single SAP Portal will improve the process for applicants, tracking and communicating the application process throughout its lifecycle. This reduces redundancies and burden on applicants that request access to data from multiple agencies. The SAP Portal will automate key tasks to save resources and time and will bring agencies into compliance with the Evidence Act statutory requirements.

Data Discovery

Individuals begin the process of accessing restricted use data by discovering confidential data assets through the SAP data catalog, maintained by federal statistical agencies at www.sap.nsf.gov. Potential applicants can search by agency, topic, or keyword to identify data of interest or relevance. Once they have identified data of interest, applicants can view metadata outlining the title, description or abstract, scope and coverage, and detailed methodology related to a specific data asset to determine its relevance to their research.

While statistical agencies and units shall endeavor to include metadata in the SAP data catalog on all confidential

data assets for which they accept applications, it may not be feasible to include metadata for some data assets (e.g., potential curated versions of administrative data). A statistical agency or unit may still accept an application even if the requested data asset is not listed in the SAP data catalog.

SAP Application Process

Individuals who have identified and wish to access confidential data assets will be able to apply for access through the SAP Portal. Applicants must create an account and follow all steps to complete the application. Applicants begin by entering their personal, contact, and institutional information, as well as the personal, contact, and institutional information of all individuals on their research team. Applicants proceed to provide summary information about their proposed project, to include project title, duration, funding, timeline, and other details including the data asset(s) they are requesting and any proposed linkages to data not listed in the SAP data catalog, including non-federal data sources. Applicants then proceed to enter detailed information regarding their proposed project, including a project abstract, research question(s), literature review, project scope, research methodology, project products, and anticipated output. Applicants must demonstrate a need for confidential data, outlining why their research question cannot be answered using publicly available information.

Submission for Review

Upon submission of their application, applicants will receive a notification that their application has been received and is under review by the data owning agency or agencies (in the event where data assets are requested from multiple agencies). At this point, applicants will also be notified that application approval does not alone grant access to confidential data, and that, if approved, applicants must comply with the data-owning agency's security requirements outside of the SAP Portal.

In accordance with the Evidence Act and the direction of the ICSP, agencies will approve or reject an application within a prompt timeframe. In some cases, agencies may determine that additional clarity, information, or modification is needed and request the applicant to "revise and resubmit" their application.

Data discovery, the SAP application process, and the submission for review are planned to take place within the web-based SAP Portal. As noted above, the renewal notice to collect

information through the SAP Portal has been published separately (90 FR 25380).

Access to Restricted Use Data

In the event of a positive determination, the applicant will be notified that their proposal has been accepted. The positive or final adverse determination concludes the SAP Portal process. In the instance of a positive determination, the data-owning agency (or agencies) will contact the applicant to provide instructions on the agency's security requirements that must be completed to gain access to the confidential data. The completion and submission of the agency's security requirements will take place outside of the SAP Portal.

Collection of Information for Data Security Requirements

In the instance of a positive determination for an application requesting access to an ERS confidential data asset, ERS will contact the applicant(s) to initiate the process of collecting information to fulfill their security requirements. These include additional requirements necessary for the statistical agency or unit to place the applicant(s) in a trusted category that may include the applicant's successful completion of identity verification, confidentiality training, nondisclosure, inspection of the site the confidential data will be accessed, and data use agreements.

ERS's data security requirements include the collection of the following information:

- *CIPSEA Training*: ERS personnel provide a Security Briefing to all applicants who were approved access to restricted data. The Briefing includes information on the Confidential Information Protection and Statistical Efficiency Act of 2018, Title III of Public Law 115–435, codified in 44 U.S.C. Ch. 35 and other applicable Federal laws that protect the restricted data. Researchers will be asked to fill out the *CIPSEA Review Form* to verify that they reviewed the training.

- Completion of form *Certification and Restrictions on the Use of Confidential ERS Data*. This form is required to be signed by researchers who have been approved to access unpublished ERS data (alternatively, some approved researchers complete on-line training in lieu of completing this form). The form contains excerpts of the various laws that apply to the unpublished data being provided to the researcher. The form explains the restrictions associated with the unpublished data and includes a place

for the researcher to sign the form, thereby acknowledging the restrictions and agreeing to abide by them.

- Completion of *ERS Site Inspection Checklist*. Researchers approved to access unpublished ERS data do so using a secure data enclave environment accessible at their own location. An ERS employee performs a site inspection (either in-person or via a video call) of the researcher's location prior to the researcher being granted access to the unpublished data. During the site inspection, the ERS employee administers the form *ERS Site Inspection Checklist*, which asks questions pertaining to the suitability of the location for restricted data access and some of the policies associated with accessing the restricted data. The form also collects information about the computer the researcher will use to access the ERS data enclave.

- Completion of *ERS Memorandum of Understanding (MOU)*. Researchers approved to access unpublished ERS data need to complete a Memorandum of Understanding Agreement between the Economic Research Service and their university, institution, or agency. The form establishes data access protocols and party responsibilities. If necessary, researchers may request an extension to their MOU using the *Extension of MOU Request Form*.

- If a researcher wishes to add a new researcher to their previously approved project, they can fill out the *Amendment for New Collaborators*. If a researcher wishes to change the scope of a previously approved project, they may fill out the *Request for Amended Project Agreement Form*. For administrative changes such as personnel, additional versions of the data, and time extensions, the researcher can fill out the *Addendum to Access Agreement*.

Specifically, researchers will be required to complete the OF–306 (Declaration for Federal Employment) to support onboarding into USDA's human capital management system. This step is necessary to establish a formal relationship between ERS and the researcher and to ensure compliance with federal identity verification and personnel tracking requirements. The OF–306 collects administrative PII such as Social Security Number (SSN), date of birth, sex, and citizenship. This information will be submitted directly to REE Onboarding and will not be retained or processed by ERS. The collection and maintenance of this data are governed by USDA's Privacy Act System of Records Notice (SORN) OCFO/NFC–1—Systems for Personnel, Payroll, and Time & Attendance (89 FR 5481, January 29, 2024). The OF–306 is

approved under OMB Control No. 3206–0182. As such, burden associated with completing the OF–306 is not included in this ICR.

Estimate of Burden: The amount of time to complete the agreements and other paperwork that comprise ERS's security requirements will vary based on the confidential data assets requested and the access modality. To obtain access to ERS confidential data assets, it is estimated that the average time to complete and submit ERS data security agreements and other paperwork is 110 minutes. This estimate does not include the time needed to complete and submit an application within the SAP Portal. All efforts related to SAP Portal applications occur prior to and separate from ERS's effort to collect information related to data security requirements.

The expected number of applications in the SAP Portal that receive a positive determination from ERS in a given year may vary. Overall, per year, ERS estimates it will collect data security information for 20 application submissions that received a positive determination within the SAP Portal. ERS estimates that the total burden for the collection of information for data security requirements over the course of the three-year OMB clearance will be about 110 hours and, as a result, an average annual burden of 37 hours.

Below we provide projected average estimates for the next three years:

Total Requests: 20.

Frequency of Request: Once per request.

Average Minutes per Request: 110 minutes.

Total Estimated Burden Hours: 37.

Comments: Comments are invited on (a) whether the proposed collection of information is necessary for the proper performance of the functions of ERS, including whether the information will have practical utility; (b) the accuracy of ERS's estimate of the burden of the proposed collection of information; (c) ways to enhance the quality, use, and clarity of the information for respondents, including through the use of automated collection techniques or other forms of information technology; and (d) ways to minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

Kelly Maguire,

Administrator, Economic Research Service,
United States Department of Agriculture.

[FR Doc. 2026–17929 Filed 9–1–26; 8:45 am]

BILLING CODE 3410–18–P

DEPARTMENT OF AGRICULTURE

Food Safety and Inspection Service

[Docket No. FSIS–2026–0166]

Notice of Request To Renew an Approved Information Collection: Generic Clearance for the Collection of Qualitative Feedback on Agency Service Delivery

AGENCY: Food Safety and Inspection Service (FSIS), U.S. Department of Agriculture (USDA).

ACTION: Notice and request for comments.

SUMMARY: In accordance with the Paperwork Reduction Act of 1995 and Office of Management and Budget (OMB) regulations, FSIS is announcing its intention to request renewal of the approved information collection regarding qualitative customer and stakeholder feedback on service delivery by FSIS. There are no changes to the information collection. The current approval will expire on May 31, 2027.

DATES: Submit comments on or before November 2, 2026.

ADDRESSES: FSIS invites interested persons to submit comments on this **Federal Register** notice. Comments may be submitted by one of the following methods:

- **Federal eRulemaking Portal:** This website provides commenters the ability to type short comments directly into the comment field on the web page or to attach a file for lengthier comments. Go to <https://www.regulations.gov/>. Follow the online instructions at that site for submitting comments.

- **Mail:** Send to Docket Clerk, U.S. Department of Agriculture, Food Safety and Inspection Service, 1400 Independence Avenue SW, Mailstop 3758, Washington, DC 20250–3700.

- **Hand- or courier-delivered submittals:** Deliver to 1400 Independence Avenue SW, Jamie L. Whitten Building, Room 350–E, Washington, DC 20250–3700.

Instructions: All items submitted by mail or electronic mail must include the Agency name and docket number FSIS–2026–0166. Comments received in response to this docket will be made available for public inspection and posted without change, including any personal information, to <https://www.regulations.gov/>.

Docket: For access to background documents or comments received, call (202) 286–2255 to schedule a time to visit the FSIS Docket Room at 1400 Independence Avenue SW, Washington, DC 20250–3700.

FOR FURTHER INFORMATION CONTACT: Gina Kouba, Office of Policy and Program Development, Food Safety and Inspection Service, USDA, 1400 Independence Avenue SW, Mailstop 3758, South Building, Washington, DC 20250–3700; 202–720–5046.

SUPPLEMENTARY INFORMATION:

Title: Generic Clearance for the Collection of Qualitative Feedback on Agency Service Delivery.

OMB Number: 0583–0151.

Type of Request: Renewal of an approved information collection.

Abstract: FSIS has been delegated the authority to exercise the functions of the Secretary (7 CFR 2.18 and 2.53), as specified in the Federal Meat Inspection Act (FMIA) (21 U.S.C. 601, *et seq.*), the Poultry Products Inspection Act (PPIA) (21 U.S.C. 451, *et seq.*), and the Egg Products Inspection Act (EPIA) (21 U.S.C. 1031, *et seq.*). These statutes mandate that FSIS protect the public by verifying that meat, poultry, and egg products are safe, wholesome, and properly labeled.

FSIS is requesting renewal of the approved information collection regarding qualitative customer and stakeholder feedback on service delivery by FSIS. There are no changes to the existing information collection. The approval for this information collection will expire on May 31, 2027.

The proposed information collection provides a means for FSIS to obtain qualitative customer and stakeholder feedback in an efficient and timely manner, consistent with the Agency's commitment to improving service delivery.

“Qualitative feedback,” refers to information that provides insights into perceptions and opinions but is not a statistical survey that yields quantitative results that can be generalized to the population studied. This feedback helps FSIS understand customer or stakeholder experiences and expectations, identify early concerns with service delivery, and highlight areas where better communication or operational changes may improve services. This collection supports ongoing, collaborative, and actionable communications between the Agency and its customers and stakeholders and directly informs improvements in program management.

The solicitation of qualitative feedback will target topics such as timeliness, appropriateness, accuracy of information, courtesy, efficiency of service delivery, and resolution of issues with service delivery. Responses will be assessed to plan and inform efforts to improve or maintain the