



NATIONAL SCIENCE FOUNDATION

Agency Information Collection Activities: Comment Request

AGENCY: National Center for Science and Engineering Statistics within the National Science Foundation.

ACTION: Submission for OMB review; comment request.

SUMMARY: The National Center for Science and Engineering Statistics (NCSES) within the National Science Foundation (NSF) has submitted the following information collection request to OMB for review and clearance under the Paperwork Reduction Act of 1995. This is the second notice for public comment; the first was published in the Federal Register at 87 FR 65611 and no comments were received. NCSES is forwarding the proposed Data Security Requirements for Accessing Confidential Data information collection to the Office of Management and Budget (OMB) for clearance simultaneously with the publication of this second notice. The full submission may be found at: <http://www.reginfo.gov/public/do/PRAMain>.

DATES: Written comments on this notice must be received by **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]** to be assured of consideration. Comments received after that date will be considered to the extent practicable. Send comments to the address below.

Comments: Comments are invited on (a) whether the collection of information is necessary for the proper performance of the functions of NCSES, including whether the information will have practical utility; (b) the accuracy of NCSES estimate of the burden of the proposed collection of information; (c) ways to enhance the quality, use, and clarity of the information on 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.

FOR FURTHER INFORMATION CONTACT: Suzanne H. Plimpton, Reports Clearance Officer, National Science Foundation, Randolph Building, 401 Dulany Street, Alexandria, VA 22314; telephone (703) 292-7556; or send email to splimpto@nsf.gov. Individuals who use a telecommunications device for the deaf (TDD) may call the Federal Information Relay Service (FIRS) at 1-800-877-8339, which is accessible 24 hours a day, 7 days a week, 365 days a year (including Federal holidays).

NSF may not conduct or sponsor a collection of information unless the collection of information displays a currently valid OMB control number, and the agency informs potential persons who are to respond to the collection of information that such persons are not required to respond to the collection of information unless it displays a currently valid OMB control number.

SUPPLEMENTARY INFORMATION:

The Foundations for Evidence-Based Policymaking Act of 2018 (Public Law 115-435, § 3583) mandates that the Office of Management and Budget (OMB) establish a Standard Application Process (SAP) for requesting access to certain confidential data assets. While the adoption of the SAP is required for statistical agencies and units designated under the Confidential Information Protection and Statistical Efficiency Act of 2018 (Pub. L. 115-435, 132 Stat. 5529), it is recognized that other agencies and organizational units within the Executive branch may benefit from the adoption of the SAP to accept

applications for access to confidential data assets. The SAP is a process through which agencies, the Congressional Budget Office, State, local, and Tribal governments, researchers, and other individuals, as appropriate, may apply to access confidential data assets held by a federal statistical agency or unit for the purpose of developing evidence. With the Interagency Council on Statistical Policy (ICSP) as advisors, the entities upon whom this requirement is levied worked with the SAP Project Management Office (PMO) and with OMB to implement the SAP. The SAP Portal is a single web-based common application for requesting access to confidential data assets from federal statistical agencies and units. The information collected through the SAP Portal is an approved information collection under OMB control number 3145-0271.

Once an application for confidential data is approved through the SAP Portal, NCSES collects information to meet its data security requirements. This collection occurs outside of the SAP Portal.

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

OMB Control Number: 3145-0278.

Type of Request: Intent to seek approval for a renewal to collect information to fulfill NCSES's security requirements allowing individuals to access confidential data assets for the purposes of building evidence.

Abstract: Title III of the Foundations for Evidence-Based Policymaking Act of 2018 (hereafter referred to as the Evidence Act) (Pub. L. 115-435, 132 Stat. 5529) 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 process was 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 the 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, NCSES is required by law to maintain careful controls that allow it to minimize disclosure risk while protecting confidentiality and privacy. The fulfillment of NCSES's data security requirements places a degree of burden on individuals, which is outlined below.

The SAP Portal is a web-based application to allow individuals to request access to confidential data assets from federal statistical agencies and units. The objective of the SAP Portal is to broaden 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) 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 NCSES uses to collect information fulfilling its data security requirements.

The SAP Policy

At the recommendation of the ICSP, the SAP Policy established the SAP to be implemented by statistical agencies and units and incorporate 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 was issued in December of 2022 as OMB memorandum M-23-04.

The SAP Portal

The SAP Portal is an application interface connecting applicants seeking data with a catalog of metadata for data assets owned by the federal statistical agencies and units. The SAP Portal is not a new data repository or warehouse; confidential data assets continue to be stored in secure data access facilities owned and hosted by the federal statistical agencies and units. The Portal provides a streamlined application process across agencies, reducing redundancies in the application process.

Submission for Review

In accordance with the Evidence Act and the SAP Policy (OMB M-23-04), 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.

Access to Restricted Use Data

In the event of a positive determination, the applicant is 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) contacts the applicant to provide instructions on the agency’s security requirements that must be completed by the

applicant to gain access to the confidential data. The completion and submission of the agency's security requirements 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 NCSES-owned confidential data asset, NCSES contacts the applicant(s) to initiate the process of collecting information to fulfill its data security requirements. This process allows NCSES to place the applicant(s) in a trusted access category and includes the collection of the following information from applicant(s):

- Restricted-use licensing agreement – This document is an agreement between NCSES and the applicant's organization provisioning NCSES's confidential data assets exclusively for statistical purposes in accordance with the terms and conditions stated in the agreement and all prevailing laws and regulations. The agreement requires signatures from the applicant(s) and a senior official at the applicant's organization who has the authority to enter the organization into a legal agreement with NCSES.
- Security plan form – This document requests information from the applicant(s) to ensure the confidential data assets are protected from unauthorized access, disclosure, or modification. The information collected in the security plan form includes the following:
 - planned work location address(es),
 - workstation specifications (make, model, serial number, type, and operating system),
 - workstation authorized users,
 - workstation monitor position (to prevent unauthorized viewing), and
 - workstation antivirus brand and version.

- Affidavit of nondisclosure form – This document describes the confidentiality protections the applicant(s) must uphold and the penalties for unauthorized access or disclosure. The form requires signatures from the applicant(s) and the principal researcher for the project as well as the imprint of a notary public.
- Rules of behavior agreement – The intent of this document is for each licensed individuals to expressly acknowledge receipt and understanding of physical security requirements and user responsibilities for devices used to access NCSES's virtual secure data access facility on an annual basis. This serves as an annual reminder and administrative safeguard in deterring improper disclosure and use of NCSES's restricted-use data.
- Individual data use agreement – The intent of this document is for each licensed individuals to expressly acknowledge receipt and understanding that NCSES restricted-use data may only be used for the following purposes under CIPSEA: data processing, statistical analysis, and statistical reporting on an annual basis. This serves as an annual reminder and administrative safeguard in deterring improper disclosure and use of NCSES's restricted-use data.

Estimate of Burden

The amount of time to complete the agreements and other paperwork that comprise NCSES's security requirements will vary based on the confidential data assets requested. The 60-day FRN specified 30 minutes of burden per applicant to complete security paperwork. This estimate has been updated to reflect an additional 30 minutes of required CIPSEA training, for a total of 60 minutes of burden per new applicant. 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 NCSES'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 NCSES in a given year may vary. Overall, per year, NCSES estimates it will collect data security information for 20 application submissions that received a positive determination within the SAP Portal as well as 90 data users who are required to complete CIPSEA training and other paperwork to continue their data access. NCSES 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 219 hours and, as a result, an average annual burden of 73 hours.

Dated: June 5, 2026.

Suzanne H. Plimpton,

Reports Clearance Officer,

National Science Foundation.

[FR Doc. 2026-11527 Filed: 6/8/2026 8:45 am; Publication Date: 6/9/2026]