This document is scheduled to be published in the Federal Register on 05/12/2023 and available online at **federalregister.gov/d/2023-10121**, and on **govinfo.gov**

7555-01-P

NATIONAL SCIENCE FOUNDATION

Agency Information Collection Activities; Comment Request; Data Security Requirements for Accessing Confidential Data

AGENCY: National Center for Science and Engineering Statistics, 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 requirement 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 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 and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to www.reginfo.gov/public/do/PRAmain. Find this particular information collection by selecting “Currently under 30-day Review – Open for Public Comments” or by using the search function.

FOR FURTHER INFORMATION CONTACT: Suzanne H. Plimpton, Reports Clearance Officer, National Science Foundation, 2415 Eisenhower Avenue, Alexandria, VA 22314, 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). Comments regarding this information collection are best assured of having their full effect if received within 30 days of this notification. Copies of the submission(s) may be obtained by calling 703-292-7556.

COMMENTS*:* Comments regarding (a) whether the proposed collection of information is necessary for the proper performance of the functions of the NSF, including whether the information shall have practical utility; (b) the accuracy of the NSF's estimate of the burden of the proposed collection of information; (c) ways to enhance the quality, use, and clarity of the information on respondents; 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 should be addressed to the points of contact in the **FOR FURTHER INFORMATION CONTACT** section.

SUPPLEMENTARY INFORMATION: NCSES 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.

Comments: Comments regarding (a) whether the collection of information is necessary for the proper performance of the functions of the NSF, including whether the information will have practical utility; (b) the accuracy of the NSF's estimate of the burden of the proposed collection of information; (c) ways to enhance the quality, use, and clarity of the information to be collected, including

through the use of automated collection techniques or other forms of information technology; (d) ways to minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated or other forms of information technology should be addressed to the points of contact in the FOR FURTHER INFORMATION CONTACT section.

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

OMB Control Number: 3145-NEW.

Summary of Collection: Title III of the Foundations for Evidence-Based Policymaking Act of 2018 (44 U.S.C. 3583; hereafter referred to as the Evidence Act) mandates that 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 (CIPSEA), 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 purposes of developing evidence. With the Interagency Council on Statistical Policy (ICSP) as advisors, the entities upon whom this requirement is levied are working with the SAP Project Management Office (PMO) and with OMB to implement the SAP.

The SAP Portal is a single web-based common application designed to collect information from individuals requesting access to confidential data assets from federal statistical agencies and units. When an application for confidential

data is approved through the SAP Portal, NCSES will collect information to fulfill its data security requirements. This is a required step before providing the individual with access to restricted use microdata for the purpose of evidence building. NCSES's data security agreements and other paperwork, along with the corresponding security protocols, allow NCSES to maintain careful controls on confidentiality and privacy, as required by law. NCSES' collection of data security information will occur outside of the SAP Portal.

The following bullets outline the major components and processes in and around the SAP Portal, leading up to NCSES' collection of security requirements.

- *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 SAP Policy was submitted to the public for comment in January 2022 (87 FR 2459) and has since been issued by OMB (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 will continue to be stored in secure data access facilities owned and hosted by the federal statistical agencies and units. The Portal will provide a streamlined application process across agencies, reducing redundancies in the application process.
- *Data Discovery*: Individuals begin the process of accessing restricted use data by discovering confidential data assets through the SAP metadata catalog, maintained by federal statistical agencies at www.researchdatagov.org.

- *SAP Application*: Individuals who have identified and wish to access confidential data assets are able to apply for access through the SAP Portal. Applicants must create an account and follow all steps to complete the application. Applicants enter personal, contact, and institutional information for the research team and provide summary information about their proposed project.
- *Submission for Review*: Agencies approve or reject an application within a prompt timeframe. Agencies may also request applicants to revise and resubmit their application.
- *Access to Confidential Data*: Approved applicants are notified through the SAP Portal that their proposal has been accepted. This concludes the SAP Portal process. Agencies will contact approved applicants to initiate completion of their security documents. 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 NCSES-owned confidential data asset, NCSES will contact 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.

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. To obtain access to NCSES confidential data assets, it is estimated that the average time to complete and submit NCSES's data security agreements and other paperwork is 60 minutes. This burden

estimate has changed from the time of the 60-day FRN submission to account for 30 minutes of CIPSEA training required for each applicant. This estimate does not include the time needed to complete and submit an application within the SAP Portal. An additional burden estimate for application renewals has also been added to account for 35 minutes of annual burden when renewing an application. 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, with two applicants per application, that received a positive determination within the SAP Portal. 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 120 hours and, as a result, an average annual burden of 40 hours.

In addition, individuals must renew applications annually and take annual CIPSEA training. An average of 90 applicants per year renew their applications, taking an average of 35 minutes for training and completion of the amendment form for a total of 157.5 total burden hours over the course of the three-year OMB clearance and an annual burden of 52.5 hours.

Comments: As required by 5 CFR 1320.8(d), comments on the information collection activities as part of this study were solicited through the publication of a 60-Day Notice in the Federal Register at 87 FR 65611. NCSES received no comments.

Updates: The 30-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 applicant. In addition, the burden estimate has been updated to account for application renewals, for a total of 35 minutes of burden per applicant.

Dated: May 8, 2023.

Suzanne H. Plimpton,

Reports Clearance Officer,

National Science Foundation.

[FR Doc. 2023-10121 Filed: 5/11/2023 8:45 am; Publication Date: 5/12/2023]