SUPPORTING STATEMENT FOR DATA SECURITY REQUIREMENTS FOR ACCESSING RESTRICTED DATA

A. JUSTIFICATION

Overview

The Foundations for Evidence-Based Policymaking Act of 2018 (44 U.S.C. 3583) mandates that the Director of 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 (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 to be 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 to be a single web-based common application designed to collect information from individuals requesting access to confidential data assets from federal statistical agencies and units. BJS makes the microdata it is required to protect as confidential available to approved researchers through a restricted access setting via its official criminal justice data archive. As a Federal Statistical Agency, BJS adheres to the SAP requirements and BJS restricted (confidential) microdata are available for discovery and application via the SAP Portal.

In June 2025, the National Center for Science and Engineering Statistics (NCSES), in its role as the SAP PMO, published a 60-day Federal Register Notice (90 FR 25380) and 30-day Federal Register Notice (90 FR 47350) announcing plans to collect information through the SAP Portal. This collection request was submitted to the OMB as a Common Form in October 2025; the OMB control number for SAP Portal information collection is 3145-0271 and the expiration date is 12/31/2028.

Each of the statistical agencies and units requiring applications through the SAP Portal submitted a request to OMB to use the NCSES Common Form. The Bureau of Justice Statistics (BJS) received this approval on 12/10/2025 and the expiration date is 12/31/2028.

When an application for BJS restricted microdata is approved through the SAP Portal, BJS will collect additional information to fulfill its data security requirements. This is a required step before providing the individual with access to restricted microdata for the purpose of evidence building. BJS data security agreements and other required security documentation and assurances along with the corresponding security protocols, allow BJS to maintain careful

controls on confidentiality and privacy, as required by law. Some of this collection will occur inside of the SAP Portal during the application process (required pre-approval documents) and other requirements will be collected outside of the SAP Portal (required post-approval documents.

This submission requests approval to collect information from individuals to fulfill BJS's data security requirements. This request is from BJS within the Office of Justice Programs, in the U.S. Department of Justice.

1. Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection. Attach a copy of the appropriate section of each statute and regulation mandating or authorizing the collection of information.

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. BJS makes its confidential data available through restricted data access via the U.S. Census Bureau's Federal Statistical Research Data Centers (FSRDC) and BJS's official data archive, currently the National Archive of Criminal Justice Data.

Data collected, accessed, or acquired by statistical agencies and units are 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, and policymakers and program managers at the local, State, Tribal, and National levels. The many benefits of access to data for evidence building notwithstanding, BJS is required by law to uphold rigorous controls that allow it to minimize disclosure risk and protect confidentiality. The fulfillment of BJS'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. BJS will collect some information related to confidentiality and data security protections during the application process in the SAP Portal (required pre-approval documents). Once an individual's application in the SAP Portal has received a positive determination, BJS will begin the process of collecting additional required information to fulfill its data security requirements (required post-approval documents).

This Paperwork Reduction Act (PRA) supporting statement outlines the SAP Policy, the steps to complete an application through the SAP Portal, and the process BJS uses to collect information to fulfill its 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 may be found in OMB Memorandum 23-04.

Method of Collection

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. BJS will continue to make its restricted data available via secure access through the Census Bureau's FSRDCs and BJS's official data archive, currently the NACJD. The 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 who 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 searching the metadata catalog on the SAP Portal. . 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 information in the SAP metadata 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 special tabulations of administrative data). A statistical agency or unit may still accept an application through the SAP Portal even if the requested data asset or special tabulation is not listed in the SAP metadata catalog.

SAP Application – Researcher Information
Individuals who have identified and wish to access confidential data assets can 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 for all individuals on their research team.

SAP Application – Research Description
Applicants provide summary information about their proposed project to include project title, duration, funding, and timeline. Other details provided by applicants include the data asset(s) they are requesting and any proposed linkages to data not listed in the SAP metadata catalog, including non-federal data sources. Applicants then enter detailed information regarding their proposed project, including a project abstract, research question(s), list of references, research methodology, project products, and requested output. Within the application, applicants must demonstrate a need for confidential data, outlining why their research question cannot be answered using publicly available information.

SAP Application – Confidentiality and Privacy Requirements
BJS will collect some data security documentation related to confidentiality and privacy processes through the SAP Portal to review an application for restricted microdata (required pre-approval documents). Once an application for restricted data is approved through the SAP Portal, BJS will collect additional information to complete its data security requirements (required post-approval documents which are described below in *Collection of Information for Data Security Requirements*).

BJS will collect documentation through the SAP Portal when an application for restricted data is submitted **(see Attachment A).** The required pre-approval documents are:

- **Privacy Certificate** – The Office of Justice Programs regulations at 28 C.F.R. Part 22 require that a Privacy Certificate be submitted as part of any application for a project in which information identifiable to a private person will be collected, analyzed, or otherwise used for research or statistical purposes. The Privacy Certificate describes the specific technical, administrative, and physical controls and procedures that will be used to protect data confidentiality and safeguard the data from misuse or unauthorized access. The Privacy Certificate is an applicant's certification to comply with BJS's confidentiality requirements. All individuals who will have access to the confidential BJS data are required to sign a Privacy Certificate to affirm their understanding of and agreement to comply with BJS's confidentiality requirements.

- **Institutional Review Board (IRB) documentation** – Users of BJS restricted data must comply with Department of Justice regulations at 28 C.F.R. Part 46 (Protection of Human Subjects), including ensuring that adequate protections are in place to protect the confidentiality of information identifiable to a private person. Applicants must submit the appropriate documentation to demonstrate that an IRB has approved or exempted the proposed project using BJS restricted data in accordance with the requirements in 28 C.F.R. Part 46. BJS's requirements related to human subjects protections are listed

on its website - https://bjs.ojp.gov/funding/human-subjects-and-confidentiality-requirements.

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). During the application process, applicants are informed that application approval alone does not 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, which may include a background check.

Data discovery, the SAP application process, and the submission for review take place within the web-based SAP Portal.

Access to BJS Restricted 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, BJS (or the lead agency in the event an application is submitted for multiple confidential agency data assets) will contact the applicant to provide instructions on any remaining data security requirements that must be completed by the applicant to gain access to the confidential data.

Collection of Information for Data Security Requirements
In the instance of a positive determination for an application requesting access to BJS restricted data file(s), BJS will contact the applicant(s) to initiate the process of collecting additional information to complete its data security requirements and grant final approval to grant access to the restricted data. This process allows BJS to place the applicant(s) in a trusted category. BJS's data security agreements and other paperwork along with the corresponding security protocols allow the agency to maintain careful controls on confidentiality and privacy, as required by law.

BJS will collect the following documents from an applicant outside of the SAP when an application for restricted data receives conditional approval through the SAP **(see Attachment B)**. The required post-approval documents are:

- **Restricted Data Use Agreement** – This document is an agreement between BJS's official archive (currently the National Archive of Criminal Justice Data [NACJD]), or its successor, on behalf of BJS, and the user(s) who is approved to access BJS's restricted data assets exclusively for statistical purposes, including evidence-building, in accordance with the terms and conditions stated in the agreement and all applicable federal laws and regulations. An applicant must submit the appropriate data security plan information to describe how they will protect the data from misuse and unauthorized access. The agreement describes the penalties associated with the misuse

or unauthorized access of the data. The agreement requires signature from the applicant(s) and any other representative who has the authority to enter into a legal agreement with NACJD, as applicable.

- **Data Security Plan** – This document describes the data access modality requested (physical enclave, virtual enclave, or secure download) and the specific data security measures and technical, physical, and administrative controls that will be followed to protect data from unauthorized disclosure and misuse.

- **Confidentiality Pledge** – This document describes the applicant's responsibilities related to accessing restricted data and confidentiality protections the applicant(s) must uphold, including adhering to applicable federal laws and regulations. The assurance requires signature from the applicant(s) and certifies their understanding of and agreement to fulfill the terms in the data use agreement and data security plan.

- **Certification of training** – Users of BJS restricted data will be required to complete relevant data security, confidentiality, and/or privacy training.

Authorization
This collection is authorized by 34 U.S.C. Section 10132. BJS is also authorized to administer some of its data collections under a different statute for the purposes described therein, for example the Prison Rape Elimination Act (PREA) (Pub. Law No. 108-79).

2. Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection.

The Paperwork Reduction Act (PRA) seeks to maximize the usefulness of information created, collected, maintained, used, shared, and disseminated by or for the federal government while also ensuring the greatest possible public benefit from such information. Additionally, the PRA mandates that the disposition of information by or for the federal government is consistent with laws related to privacy and confidentiality. BJS's data security requirements ensure that BJS is compliant with PRA and its other statutory requirements.

Data collected, accessed, or acquired by statistical agencies and units are vital for developing evidence on conditions, characteristics, and behaviors of the public and on the operations and outcomes of public programs and policies. Access to confidential data on businesses, households, and individuals from federal statistical agencies and units enables agencies, the Congressional Budget Office, State, local, and Tribal governments, researchers, and other individuals to contribute evidence-based information to research and policy questions on economic, social, and environmental issues of national, regional, and local importance. 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.

Many applicants will be academic research faculty or students at U.S. universities or other types of research institutions. Other applicants are likely to include analysts at nonprofit organizations and research groups in U.S. Government organizations (Federal, State, local, and Tribal). Scientific research typically results in papers presented at scientific conferences and published in peer-reviewed academic journals, working paper series, monographs, and technical reports. The scientific community at large benefits from the additions to knowledge resulting from research with statistical agencies and units' data. Results inform both scientific theory and public policy and can assist agencies in carrying out their missions.

Approved applicants using confidential data can provide insights on how statistical agencies and units may improve the quality of the data collected or acquired; identify shortcomings of current data collection programs and data processing methods; document new data needs; and develop methods to address survey nonresponse or improve statistical weights.

3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses, and the basis for the decision for adopting this means of collection. Also, describe any consideration of using information technology to reduce burden.

BJS will contact individuals via email whose applications for restricted data are approved to request additional documentation to satisfy BJS's data security requirements prior to granting access to the data. For documentation that will be submitted outside of the SAP, applicants will submit the required form via email to BJS's official archive, currently NACJD.

4. Describe efforts to identify duplication. Show specifically why any similar information already available cannot be used or modified for use for the purposes described in Item A.2 above.

BJS is required by law to maintain careful controls on confidentiality and limit disclosure risk. Its data security forms are required for each approved research project to ensure minimal disclosure risk of BJS restricted data. BJS has reviewed its data security requirements to eliminate duplication.

5. If the collection of information impacts small business or other small entities, describe any methods used to minimize burden.

Small businesses or their representatives may be among those who choose to apply for BJS restricted data through the SAP. The burden of this collection does not represent a significant barrier to participation from small businesses and is not large enough to pose significant costs to respondents, including small businesses.

6. Describe the consequence to federal program or policy activities if the collection is not conducted or is conducted less frequently, as well as any technical or legal obstacles to reducing burden.

BJS requires and collects information for its data security forms for all individuals who will access data and output that has not been cleared for disclosure review. Less frequent collection would compromise BJS's ability to secure its restricted data.

7. Explain any special circumstances that would cause an information collection to be conducted in a manner:

- **requiring respondents to report information to the agency more often than quarterly;**
- **requiring respondents to prepare a written response to a collection of information in fewer than 30 days after receipt of it;**
- **requiring respondents to submit more than an original and two copies of any document;**
- **requiring respondents to retain records, other than health, medical, government contract, grant-in-aid, or tax records for more than three years;**
- **in connection with a statistical survey, that is not designed to produce valid and reliable results that can be generalized to the universe of study;**
- **requiring the use of statistical data classification that has not been reviewed and approved by OMB;**
- **that includes a pledge of confidentially that is not supported by authority established in statute or regulation, that is not supported by disclosure and data security policies that are consistent with the pledge, or which unnecessarily impedes sharing of data with other agencies for compatible confidential use; or**
- **requiring respondents to submit proprietary trade secret, or other confidential information unless the agency can demonstrate that it has instituted procedures to protect the information's confidentially to the extent permitted by law.**

There are no special circumstances.

8. If applicable, provide a copy and identify the date and page number of publication in the Federal Register of the agency's notice, required by 5 CFR 1320.8(d), soliciting comments on the information collection prior to submission to OMB. Summarize public comments received in response to that notice and describe actions taken by the agency in response to these comments. Specifically address comments received on cost and hour burden.

Describe efforts to consult with persons outside the agency to obtain their views on the availability of data, frequency of collection, the clarity of instructions and recordkeeping, disclosure, or reporting format (if any), and on the data elements to be recorded, disclosed, or reported.

On February 6, 2026, BJS published a 60-day notice in the Federal Register (91 FR 5513) inviting the public and other federal agencies to comment on plans to submit this request. BJS received no comments. The 30-day notice was published on April 7, 2026 (91 FR 17663).

9. Explain any decision to provide any payments or gifts to respondents, other than remuneration of contractors or grantees.

No payments or gifts are given to holders of user accounts in the system.

10. Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation or agency policy.

BJS is authorized to conduct this data collection under 34 U.S.C. § 10132. BJS will protect and maintain the confidentiality of the personally identifiable information (PII) it collects to the fullest extent under federal law. BJS will report the information collected through the SAP Portal in accordance with the reporting requirements in the SAP Policy.

11. Provide additional justification for any questions of a sensitive nature, such as sexual behavior and attitudes, religious beliefs, and other matters that are commonly considered private. This justification should include the reasons why the agency considers the questions necessary, the specific uses to be made of the information, the explanation to be given to persons from whom the information is requested, and any steps to be taken to obtain their consent

Not applicable. The SAP application materials do not contain questions of a sensitive nature.

12. Provide estimates of the hour burden of the collection of information. The statement should:

- **Indicate the number of respondents, frequency of response, annual hour burden, and an explanation of how the burden was estimated. Unless directed to do so, agencies should not conduct special surveys to obtain information on which to base hour burden estimates. Consultation with a sample (fewer than 10) of potential respondents is desirable. If the hour burden on respondents is expected to vary widely because of differences in activity, size, or complexity, show the range of estimated hour burden, and explain the reasons for the variance. General, estimates should not include burden hours for customary and usual business practices.**
- **If this request for approval covers more than one form, provide separate hour burden estimates for each form.**
- **Provide estimates of annualized cost to respondents for the hour burdens for collections of information, identifying and using appropriate wage rate categories. The cost of contracting out or paying outside parties for information collection**

activities should not be included here. Instead, this cost should be included in Item 14.

The amount of time to complete the agreements and other paperwork that comprise BJS data security requirements will vary based on the restricted data assets requested. To obtain access to BJS restricted data assets, it is estimated that the average time to complete and submit BJS data security agreements and other paperwork is 3 hours (180 minutes). This estimate does not include the time needed to complete and submit other required application materials within the SAP Portal.

The expected number of applications in the SAP Portal that receive a positive determination from BJS in a given year may vary. Overall, per year, BJS estimates it will collect data security information for 55 application submissions that received a positive determination within the SAP Portal. BJS 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 495 hours and, as a result, an average annual burden of 165 hours.

The total cost to complete BJS's data security requirements for the 3 total burden hours is estimated to be $120 per applicant.. This estimate is based on an estimated median annual salary of $83,500 per applicant.[1] Assuming a 40-hour workweek and a 52-week salary, this annual salary translates to an hourly salary of $40.14. Over the three-year OMB clearance period, the cost to the public for BJS's security forms is estimated to be $19,869 ($40.14 per hour x 495 hours). See Table 1 for details.

Table 1. Estimated Annualized Respondent Cost and Hour Burden

Activity	Number of respondents	Total annual responses	Time per response	Total burden hours	Hourly rate[2]	Monetized value of respondent time (burden hours x hourly rate)
Data security requirements and paperwork						
Fiscal Year 2026	55	55	180 mins	165 hours	$40.14	$6,623.10
Fiscal Year 2027	55	55	180 mins	165 hours	$40.14	$6,623.10
Fiscal Year 2028	55	55	180 mins	165 hours	$40.14	$6,623.10
Total costs for 3-year period	**165 respondents**	**--**	**--**	**495 hours**	**--**	**$19,869.30**

[1]Applicant salary estimates were based on annual median salary estimates for employed college graduates using data from the 2023 National Survey of College Graduates.

[2]Based on annual median salary estimates for employed college graduates using data from the 2019 National Survey of College Graduates. Accessed April 7, 2026.

13. Provide an estimate of the total annual cost burden to respondents or recordkeepers resulting from the collection of information. (Do not include the cost of any hour burden shown in Items 12 and 14).

- **The cost estimate should be split into two components: (a) a total capital and start up cost component (annualized over its expected useful life); and (b) a total operation and maintenance and purchase of service component. The estimates should take into account costs associated with generating, maintaining, and disclosing or providing the information. Include descriptions of methods used to estimate major cost factors including system and technology acquisition, expected useful life of capital equipment, the discount rate(s), and the time period over which costs will be incurred. Capital and start-up costs include, among other items, preparations for collecting information such as purchasing computers and software; monitoring, sampling, drilling and testing equipment; and record storage facilities.**
- **If cost estimates are expected to vary widely, agencies should present ranges of cost burdens and explain the reasons for the variance. The cost of purchasing or contracting out information collection services should be a part of this cost burden estimate. In developing cost burden estimates, agencies may consult with a sample of respondents (fewer than 10), utilize the 60-day pre-OMB submission public comment process and use existing economic or regulatory impact analysis associated with the rulemaking containing the information collection, as appropriate.**
- **Generally, estimates should not include purchases of equipment or services, or portions thereof, made: (1) prior to October 1, 1995, (2) to achieve regulatory compliance with requirements not associated with the information collection, (3) for reasons other than to provide information or keep records for the government, or (4) as part of customary and usual business or private practices.**

Not applicable. BJS does not impose any fees, charges, or costs to individuals submitting BJS security forms.

14. Provide estimates of the annualized cost to the Federal Government. Also, provide a description of the method used to estimate cost, which should include quantification of hours, operational expenses (such as equipment, overhead, printing, and support staff), any other expense that would not have been incurred without this collection of information. Agencies also may aggregate cost estimates from Items 12, 13, and 14 into a single table

We estimate the average annual cost to the Federal Government for the collection and review of BJS data security documents to be approximately $13,000 per year, for an estimated $39,000 for the 3-year period of Fiscal Years 2026, 2027, and 2028. These figures are based on required contractual and staff resources necessary to collect and review documents given the expected annual number of 55 submitted applications. See Table 2 for details.

Table 2. Cost to the Federal Government[3]

[3] SALARY TABLE 2026-DCB (opm.gov). Accessed April 7, 2026.

Items	Hourly rate	Staff total	Hours to review application	Total cost
BJS Subject Matter Experts (SME) application review (1 staff)				
1 program analyst (GS-14 step 10)	$89.65	1	1	$89.65
BJS Coordinator (1 staff)				
1 support staff (GS-12 step 1)	$49.07	1	1	$49.07
BJS Contractor Support application review (1 staff)				
1 support staff (GS-12 step 1 equivalent)	$49.07	1	2	$98.14
Total cost per application	--	--	--	**$236.86**
Total cost x 55 applications per year	--	--	--	**$13,027.30**
Total costs to BJS for 3-year period	--	--	--	**$39,082**

15. Explain the reasons for any program changes or adjustments.

BJS revised the costs downward from the last submission to more accurately reflect staff and contractor time spent solely reviewing the data security requirements.

16. For collections of information whose results will be published, outline plans for tabulations, and publication. Address any complex analytical techniques that will be used. Provide the time schedule for the entire project, including beginning and ending dates of the collection of information, completion of report, publication dates, and other actions.

The information provided by applicants to BJS is received on an ongoing basis and is not subject to any schedule. Users provide information voluntarily and at their discretion.

17. Expiration Date Approval

The expiration date of OMB approval will be displayed on BJS's data security forms.

18. Exceptions to the Certification

This collection of information does not include any exceptions to the certificate statement.

B. Collections of Information Employing Statistical Methods

Not applicable. The current request seeks to obtain approval for data security requirements from approved applicants seeking BJS restricted data assets. These documents will not employ statistical methods.