SUPPORTING STATEMENT FOR THE LAWFUL ACCESS DATA COLLECTION

The FBI requests an extension of the approved Lawful Access Data Collection under **OMB Control Number [1110-0088].** Since the collection's launch in 2024, participation has been limited. The requested extension will provide additional time to evaluate the collection's effectiveness, assess future needs, and determine the most appropriate path forward.

A. JUSTIFICATION

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.

Over the past two decades, advances in communications and digital storage technologies have significantly changed the way individuals communicate, store information, and access digital services. While these technological developments provide substantial benefits, they also create challenges for law enforcement investigations. In some instances, encryption and other technological protections prevent law enforcement from accessing data relevant to criminal investigations, even when investigators obtain the appropriate legal authority, such as a court order or search warrant.

To better understand the scope and impact of these challenges, the FBI's Uniform Crime Reporting (UCR) Program, in collaboration with the National Domestic Communications Assistance Center (NDCAC) and the Lawful Access Task Force, developed and maintain a set of data elements designed to measure instances in which lawful access to digital evidence is impeded. The Lawful Access Data Collection (LADC) serves as the mechanism for collecting information on investigations affected by device or software encryption and other access barriers.

Data collected through the LADC could help the FBI and its partners assess the extent to which lawful access challenges affect criminal investigations and informs policy, operational, and resource decisions related to these issues. The collection strives to provide decisionmakers with objective data regarding the impact of lawful access limitations on law enforcement activities and public safety.

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 LADC is designed to provide information on instances where law enforcement investigations are negatively impacted by device encryption and/or encrypted applications and software. Both cases involve the restriction of encrypted data from access by law enforcement

agencies after lawful authorization has been granted to the agency to view or access the above-mentioned data.

A primary factor for the LADC is distinguishing between the types of data encryption being encountered during an investigation. In most cases, data can be classified as one of two types: data in motion or data at rest. Understanding these data classifications is paramount to the issues surrounding lawful access disruptions. Below are the definitions for the different types of encrypted data:

- **Data in Motion**–Real-time information such as phone calls, email, text messages, and chat sessions in transit.
- **Data at Rest**–Data stored on devices, such as email, text messages, application data, photos, and videos.

These types of encrypted data are the focus of LADC. The collection of data elements depend greatly on the type of encrypted data encountered during the reported incident.

The LADC contains two separate portions, the first specific to the collection of agency/case information, and the other specific to the collection of encrypted device/encrypted application(s)/software information. This layout is designed to allow agencies to provide the most granular information possible regarding gathered devices, which form the basis of lawful access information, while also streamlining the collection instrument as much as possible. Major data collected are:

- Agency information, such as originating agency identifier
- Associated criminal act with encryption report
- Type of device or application/software
- Date of device seizure or application/software reporting
- Version of device operating system
- Association of device or application/software with offender, victim, or both
- Outcome of access attempt

For a more detailed look at the collection instrument and the question forms, please review the collection instrument attached to this clearance request package.

This information will serve as the basis for an evaluation of the volume of law enforcement cases affected by device and application encryption and will provide a range of potential customers with the ability to analyze statistical metrics and data points associated with these types of instances. This information will also help to inform policy makers of important aspects of lawful access issues with the hope of crafting responsible policies to ensure both safety and privacy for the public.

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.

The LADC provides a centralized repository for the responsible law enforcement agency representatives to submit data pertaining to the impacted case to the FBI's UCR Program. The Collection of Law Enforcement and Crime Tool (COLECT) is a robust application that will enable the nation's law enforcement agencies to submit LADC information to the FBI's UCR Program. The COLECT has been created to allow agencies the use of an FBI-developed interface to submit and manage their agency's submissions to the FBI's UCR program, including participation in the LADC. Detailed information about these and other features are included within this document.

All users access the COLECT through the FBI's Law Enforcement Enterprise Portal (LEEP). COLECT uses the LEEP for authentication and the related user account to provide access to information and functionality within the software.

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.

The FBI's UCR Program worked with members of the LADC task force to identify potential areas of duplication for this collection. While the topic of lawful access and the issue of data encryption has become more salient in recent years, the actual collection and analysis of encrypted data and its effect on law enforcement activities has not been attempted on a large scale. The LADC is be the first such collection program focused on gathering this type of information.

During the evaluation process, the FBI's UCR Program worked extensively with the National Domestic Communications Assistance Center (NDCAC) to evaluate lawful access collection efforts that their agency had attempted in the past. As of 2023, NDCAC is not performing any lawful access collection efforts that would duplicate or replicate the efforts of the LADC.

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

To mitigate potential burden on all participating entities, the FBI has built the COLECT as a web portal which will serve as a platform to access the LADC application. Also, based on research conducted with the LADC task force and other federal agencies, many small agencies do not have the funds necessary to create or maintain their own digital forensics departments. This leads many small agencies to either distribute data decryption to a third-party agency, such as a state crime lab, or an outside contractor with decryption capabilities. In these cases, these small agencies would not be the primary access point for lawful access information. The FBI's UCR Program plans to continually evaluate the collection universe and primary access points to maximize accurate responses without undue burden to smaller agencies.

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.

The LADC will provide vital information on the volume of impacted law enforcement investigation along with key metrics related to data encryption and its effect on law enforcement investigations activities. The FBI's UCR Program is requesting agencies submit reports on negatively impacted cases once a delay in investigative activities that can be attributed to data encryption is determined. Not collecting this information will result in a loss of potential knowledge and decision-making abilities around the topic of lawful access and law enforcement activities.

The FBI's UCR Program is requesting law enforcement agencies submit information on an incident-by-incident basis. This means agencies will submit data on an impacted investigation after the incident has occurred. Participation in the LADC is voluntary and law enforcement agencies are under no existing requirement to submit information at any defined cadence concerning this topic.

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.**

The FBI's UCR Program is requesting law enforcement agencies submit information on an incident-by-incident basis. This means agencies will submit data on an impacted investigation after the incident has occurred. Participation in the LADC is voluntary and law enforcement agencies are under no existing requirement to submit information at any defined cadence. The LADC does not contain data elements or any additional questions that meet the special circumstances specifications found in the Paperwork Reduction Act Guide. Additionally, respondents are expected to respond to this collection 50 times annually.

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.

Consultation with representatives of those from whom information is to be obtained or those who must compile records should occur at least once every 3 years -- even if the collection-of-information activity is the same as in prior periods. There may be circumstances that may preclude consultation in a specific situation. These circumstances should be explained.

The 60-Day Notice was published in the Federal Register on September 19, 2026, (91 FR 66583). The comment period ended on November 20, 2026. One comment was received:

The commenter supports strong encryption and recommends that any approved data collection be transparent, respect privacy, track whether warrants were obtained and not be used to justify weakening encryption or requiring government access. They also question the estimate of 950,000 respondents and request an explanation of how it was calculated.

The UCR Program acknowledged the comment and explained how the estimate of respondents was calculated, referencing Item 12 in this supporting statement.

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

Not applicable.

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

The FBI's UCR Program does not assure confidentiality. However, LADC data does not contain directly identifiable information which would reveal the identity of an individual. In addition, LADC data are not expected to be released directly to the public as part of a regular release or publication by the FBI's UCR Program.

The agency case identification or number is collected in the LADC, but no other identifying information about the reporting agency or individuals involved is gathered, and the collected criminal offenses element is a list of unique offenses categories created specifically for the LADC. There is no connection between this information and any personal or sensitive information. The FBI has completed a Privacy Threshold Analysis (PTA) to identify privacy risks and mitigations pertinent to this collection. The PTA determined that this information collection presents no significant privacy risks.

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.

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.

This estimate is based on an estimated total 19,000 eligible law enforcement agencies and an estimated average response rate of 50 reported cases per agency. As the volume of cases impacted by encryption will vary based on agency size and population coverage, this average rate of response will serve as a starting point for burden estimation. As agencies begin to report information to the FBI, the FBI's UCR Program will evaluate the number of reports received to calculate more accurate metrics for annual burden. Below is a calculation of the estimated burden using a response time of 3 minutes, 12 seconds.

According to the U.S. Bureau of Labor Statistics for 2023, the mean hourly wage of law enforcement officers is $36.80. Therefore, the monetary burden is an estimated $1,864,546 (50,667 annual hours x $36.80).

Estimated Annualized Respondent Cost and Hour Burden

Activity	Number of Respondents	Frequency	Total Annual Responses	Time Per Response	Total Annual Burden (Hours)	Hourly Rate*	Monetized Value of Respondent Time
LADC	19,000	50	950,000	3 minutes 12 seconds	50,667	36.80	1,864,546

U.S. Bureau of Labor Statistics for 2023

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.**

There are no direct costs to law enforcement to participate in the FBI's UCR Program other than the time to respond to the data collection questions, and for any additional follow-up between the agency and the FBI's UCR Program. Respondents may incur capital or start-up costs associated with this information collection, although it is difficult to obtain the costs from agency-to-agency.

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.

According to the Fiscal Year (FY) 2024 cost model provided by the FBI's Criminal Justice Information Services (CJIS) Division, Resources Management Section, Financial Management Unit, the following are actuals based upon 2024 collection activity. The cost module does not separate the costs between the two methods of collecting UCR data (i.e., SRS and NIBRS).

Activity	FY2024 Annualized Cost	FY2024 Annualized Full-Time Equivalent
CJIS Systems Agency/Officer Development and Support	$4,805.07	0.03
Collaborate with LE and Critical Incident Management Services	$8,479.06	0.06
Conduct Field Office, Office and Partner Engagement, and LEGAT Engagement Activities	$18,456.52	0.15
Conduct Liaison, Education, and Promotion	$530,655.46	4.03
Conduct Other Crime Data Services Activities	$392,300.68	2.81
Conduct Other Partner Engagement Activities	$41,822.65	0.27
Conduct Quality, Process, and System Management Activities	$10,191.78	0.06
Conduct research and release studies on collected data	$221,358.28	1.79
Conduct State and Local Agency Engagement Activities	$71,379.09	0.56
Conduct Tribal Engagement Activities	$9,865.78	0.09
Develop and Maintain Partner Outreach Materials	$8,365.12	0.06

Activity–continued	FY2024 Annualized Cost	FY2024 Annualized Full-Time Equivalent
Develop and Manage Policy	$52,028.62	0.36
Direct Customer Engagement for Product/Service Use and Expansion	$156,869.82	1.03
Manage Strategic Communications	$9,212.45	0.06
Perform Administrative and Human Resource tasks	$260,597.57	1.90
Perform Advisory Policy Board (APB) tasks	$60,450.64	0.41
Perform Budget, Strategic Planning, and Program Control	$151,704.61	0.91
Perform Contracting Officer's Representative Duties	$33,935.03	0.21
Perform Quality Assurance	$160,033.71	1.24
Perform Quality Management	$16,624.04	0.10
Perform Scaled Agile Framework Duties	$457,011.19	3.81
Perform Statistical Reporting	$930.39	0.01
Perform Strategy Management	$40,890.38	0.23
Perform workload management	$16,487.43	0.09
Planning and Implementing New Data Collections	$87,978.26	0.70
Process Media, Freedom of Information Act, and Congressional requests	$79,491.70	0.53
Provide CJIS Multimedia Support	$3,159.67	0.03
Provide End User Support Services	$88,656.10	0.65
Provide Management and Administration	$532,640.20	3.36
Provide Support to Other FBI Units Sections (Temporary Duty, Surge)	$20,154.92	0.20
Respond to Data Calls, Media Requests, etc.	$260,146.69	1.91
Respond to Internal and External Data Calls	$119,149.70	0.69
Support CJIS APB	$51,763.19	0.36
Support CJIS Division Community Outreach Program	$10,105.00	0.09
Support CJIS Systems Officer Training and Communications	$3,899.61	0.03
Support *Crime in the Nation* (*CITN*) data release	$469,426.78	3.58
Support Law Enforcement Employee Counts Data Collection	$147,784.63	1.16
Support Law Enforcement Suicide Data Collection	$102,405.30	0.80
Support Law Enforcement Training	$10,572.66	0.12
Support LEOKA Collection and data release	$275,957.77	2.25
Support National Incident-Based Reporting System	$178,076.89	1.38
Support National UoF Data Collection	$206,931.23	1.72
Support Originating Agency Identifier Administration	$7,799.21	0.06
Support Reports, Releases, and Publications	$71,322.10	0.61
Support the FBI's Crime Data Explorer (CDE)	$186,781.39	1.50
Support the Hate Crime Data Collection and data release	$152,748.80	1.18
Support the Law Enforcement Public Contact Data Collection	$40,623.54	0.30

Support the Lawful Access Data Collection	$49,628.26	0.33
Support the Quarterly UCR information	$78,946.16	0.56

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

Not applicable

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.

Due to limited participation, and the existing unknowns around the total universe of participating agencies, the FBI still plans to implement a research-based publication strategy rather than a cadence-based release strategy. Instead of releasing metrics on a quarterly or annual basis, the FBI will conduct an analysis of the reported cases every three – five years, producing a detailed analysis product that will be released to the public via the CDE. The FBI will provide detailed methodology and analysis documents to support proper understanding of the metrics seen in these analysis reports and the methods used to arrive at data collection findings. As the FBI begins to receive data submissions from agencies, the FBI will continue to evaluate the proper cadence for releasing reports and other forms of LADC data.

In the time between analysis products, the FBI will develop the ability to run reports on demand to provide to internal partners and policy makers for the purpose of research and analysis that can help educate and inform internal partners with a national view of lawful access data. These reports will cover all reported data submitted to the FBI based on a determined timeframe, but no analysis will be provided. Information in these on-demand reports will carry an embargo policy to restrict public release of the information until formal release by the FBI.

Evaluation of participation and population coverage will be an area of research and analysis for the future of the LADC. The need for a study focused on the total population coverage and potential nonresponse will be evaluated after sufficient data have been collected to provide a clearer picture of the available data that exists within the LADC scope.

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain the reasons that display would be inappropriate.

The FBI does not wish to display the expiration date for OMB approval of the information collection due to the mode of data collection. The LADC will be collected via web form available on COLECT through the restricted-access LEEP. To keep an expiration date current would require constant programming changes of the web form by the FBI.

18. Explain each exception to the certification statement.

Not applicable

B. COLLECTIONS OF INFORMATON EMPLOYING STATISTICAL METHODS.

This collection does/does not contain statistical data.