Federal Bureau of Investigation

Privacy Impact Assessment
for the
[Law Enforcement Suicide Data Collection]

Issued by:
Erin M. Prest, Privacy and Civil Liberties Officer

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: June 2, 2021

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

On June 16, 2020, the President of the United States signed into law the Law Enforcement Suicide Data Collection Act (LESDCA), codified at 34 U.S.C. § 50701. The LESDCA directs the Federal Bureau of Investigation (FBI) to establish a new data collection to better understand and prevent suicides among current and former law enforcement officers (LEO)[1] at the federal, state, tribal, and local levels. The FBI's Criminal Justice Information Services (CJIS) Division, Crime Statistics Management Unit (CSMU) is establishing the Law Enforcement Suicide Data Collection (LESDC) to meet the requirements of the LESDCA to collect information about current and former law enforcement officers who commit or attempt to commit suicide. Federal, state, local, tribal, and territorial law enforcement agencies[2] will voluntarily provide the FBI with information regarding the suicides and attempted suicides committed by their law enforcement officers. The FBI will compile and publish statistical data on law enforcement suicides. Publication of the LESDC information will provide information to assist in better understanding and preventing suicides within the law enforcement community.

While the LESDC is not designed to collect directly identifiable information about LEOs who commit or attempt to commit suicide, the combination of the data elements collected might allow, in certain circumstances, LEOs involved in the incidents to be identified. This privacy impact assessment (PIA) explores the effects of the linkability of the data and the decisions made to limit, to the extent possible, the ability to indirectly identify the LEOs who commit or attempt to commit suicide. This PIA also addresses the collection of user information for individuals who report LEO suicides and attempted suicides to the LESDC.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

---

[1] The LESDCA defines "law enforcement officer" as "any current or former officer (including a correctional officer), agent, or employee of the United States, a State, Indian Tribe, or a political subdivision of a State authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of any violation of the criminal laws of the United States, a State, Indian Tribe, or a political subdivision of a State." 34 U.S.C. 50701(e)(2). For purposes of the LESDC, the term law enforcement officer will encompass public safety telecommunicators (e.g. 9-1-1 operators), prosecuting attorneys, and judges.

[2] The LESDCA defines "law enforcement agency" as "a Federal, State, Tribal, or local agency engaged in the prevention, detection, or investigation, prosecution, or adjudication of any violation of the criminal laws of the United States, a State, Tribal, or a political subdivision of a State." 34 U.S.C. 50701(e)(1). For purposes of the LESDC, the term law enforcement agency will encompass prosecuting attorneys' offices and courts.

The FBI developed the LESDC to fulfill its statutory requirements under the LESDCA. The LESDC enables agencies to submit law enforcement suicide and attempted suicide information to the Uniform Crime Reporting (UCR) Program. The LESDCA directs the FBI to collect the following information about law enforcement suicides and attempted suicides: the circumstances and events that occurred before each suicide or attempted suicide; the general location of each suicide or attempted suicide; the demographic information of each law enforcement officer who commits or attempts suicide; the occupational category, including criminal investigator, corrections officer, line of duty officer, and 911 dispatch operator, of each law enforcement officer who commits or attempts suicide; and the method used in each suicide or attempted suicide. To collect the suicide and attempted suicide data, the FBI is creating an additional report type within its NIBRS Collection Application (NCA).[3] The NCA allows law enforcement agencies and state UCR programs to submit data directly to the FBI for the LESDC.

The LESDC collects data voluntarily submitted by federal, state, local, tribal, and territorial agencies regarding current and former LEOs within their agencies who commit or attempt to commit suicide. The LESDC allows agency personnel to manually submit law enforcement suicide and attempted suicide information to the UCR Program. The LESDC is accessible via the NCA. The NCA resides on the Amazon Web Services government cloud (AWS Gov-Cloud) environment and is accessible through the Law Enforcement Enterprise Portal (LEEP).[4] Submitting agency personnel will use LEEP for authentication into the NCA. Users access the NCA on LEEP via a web browser.

To use the LESDC, the submitter authenticates into LEEP and, after receiving proper authorization to access the NCA, opens the NCA, selects the LESDC report, and submits the data. Users access LEEP through an Identity Provider (IdP).[5] When a user selects the NCA, LEEP passes the user's attributes to the NCA for authentication. Once logged in to the NCA, users can enter, save, validate, and submit incidents to the LESDC. Alternatively, a law enforcement agency with a suicide incident to report can contact the FBI and ask the UCR Program staff to enter the suicide incident information on its behalf. The FBI requests that law enforcement agencies provide suicide incident information within the publication year of the incident occurrence. Data submitted after publication cutoff will be accepted into the collection but may not be included in the current year's release. Once received, the UCR Program will use LESDC information to release statistical information on LEO suicides and attempted suicides.

To submit data to the UCR Program, agencies must have a UCR recognized originating agency

---

[3] The FBI initially developed the NCA to allow federal and tribal agencies to submit National Incident-Based Reporting System (NIBRS) incidents to the UCR program. The UCR Program is rebranding and expanding the NCA to allow agencies to submit additional types of UCR information, such as law enforcement suicide data, through the NCA. The PIA for the UCR Program discusses the NCA. The name, NIBRS Collection Application, is subject to change.

[4] LEEP is a federated gateway that securely connects law enforcement, criminal justice, and homeland security communities to applications and services over the Internet. The benefits of LEEP include a single sign-on for users to access various services and systems (such as the NCA) and ensuring that only authenticated users have access to those systems and services. LEEP has separate privacy documentation.

[5] An IdP is defined as an organization/agency that creates, maintains, and vets information about each of its authorized users for LEEP access. The IdP performs user authentication each time an individual logs in to LEEP. The IdP also assigns the current attributes about the individual for a given information technology session. These attributes are presented when the user accesses LEEP via a secure web browser session at a designated URL, which then allows users access to Service Providers, in this case the NCA and the LESDC reporting form.

identifier (ORI). Users with a valid UCR ORI can apply for account access to the NCA via LEEP. Authorized users include personnel of federal, state, tribal, and territorial government agencies with the ability to submit data to the UCR Program. Once approved for access, users are assigned a user role which controls their ability to enter, view, and manage data within the NCA, including LESDC incidents. Access to incident submissions in the LESDC is limited to authorized users.

The UCR Program controls initial NCA account access for agencies. Once the UCR Program establishes an agency point of contact in the NCA, the point of contact is assigned an Administrator role and the appropriate ORIs associated with the user's area of responsibility. Administrators serve as account managers for their agencies. As account managers, Administrators can create, approve, update, and delete roles and privileges for their users and assign roles to users. Administrators also have the functionality assigned to contributor and submitter roles.

Users assigned as incident contributors by an agency can create and update incidents on behalf of their agency, but they cannot submit incidents to the UCR Program. Users assigned the submitter role can create and update incidents on behalf of their agency as well as indicate whether an incident for their agency is complete and submit the incident to the UCR Program on behalf of their agency. Users will only have access to incidents associated with their assigned ORIs. Users can retrieve incidents by ORI, incident date, and can filter incidents by the name of the user creating the incident. Users can also view the incident history (e.g. created, modified, deleted, and reassigned) for all incidents associated with their ORIs. A user can access all incidents associated with their assigned ORIs, not just incidents they have created. All agency users will be able to download a copy of the incident submissions associated with their assigned ORIs.

FBI employees supporting the UCR Program and the LESDC can view all entries within the NCA; create an incident on behalf of a requesting agency; indicate whether an incident is complete and submit an incident for the next step of the review process; review incidents and check for data quality errors; inform data owners if the data needs to be updated; export data to spreadsheets; and view the transaction history for incidents. In addition, with the NCA, FBI users can choose data for inclusion in reports, create reports and dashboards, and export LESDC data to spreadsheets for processing, retention, and publication preparation. Exported spreadsheets with incident level data are not publicly released. Exported spreadsheets are maintained on internal FBI systems and accessible only to authorized FBI personnel supporting the LESDC. Statistical reports, charts, and graphs created from LESDC information will be pushed to the Crime Data Explorer (CDE)[6] for publication. The statistical information published will use aggregated data from incident submissions to the LESDC that will limit the ability of the reader or user to link information back to a particular LEO. See Section 4.2 for more information.

FBI database administrators are responsible for maintaining the database and can view and access the data, including LESDC data, in the NCA. FBI system administrators are responsible for maintaining the software, security, and hardware.

---

[6] The CDE is a web-based solution that enables the public to view and interact with national UCR data in an intuitive and user-friendly way. The CDE provides UCR data to the public via an interactive website that allows the general public to query, view, and download statistical crime reporting data submitted voluntarily to the national UCR Program. The PIA for the National UCR Program addresses the CDE. To access the CDE, please visit: https://crime-data-explorer.fr.cloud.gov/

Access to a specific user's information is role based and restricted to the user, other users in the user's chain of review, and FBI personnel supporting the UCR Program and the LESDC, including system and database administrators. User information is maintained to provide users and reviewers with point of contact information, to facilitate generating system reports on items such as which users and agencies have submitted data and which users and agencies have incidents that need to be reviewed or submitted, and to allow users to subscribe to system reports and alerts. The FBI will also leverage user information to provide messages from the NCA such as data submission errors, data quality messages, and other messages regarding agencies' data submission statuses.

The NCA collects audit logs on user activity within the application. Audit information is retrievable by any data element in the audit logs. Security personnel review audit logs using automated log aggregation toolsets. System security administrators (SSAs) monitor audit logs on a daily basis. The Information System Security Officer (ISSO) reviews audit logs, at a minimum, every seven days.

Incident information collected by the LESDC will be used to create statistical reports and publications to aid in preventing future law enforcement suicides and promoting the understanding of suicide in law enforcement. Statistical data from the collection will be made public. Statistical data cleared for public release will be made public through publications on the CDE. Publications will be designed to limit the ability of the reader or user to link information back to a particular LEO. As set forth in the LESDCA, publicly released information will be designed to manage the risk of identity disclosure based upon best practices identified by Federal statistical programs. In addition to statistical information released on the CDE, the FBI will provide an annual report to Congress.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority		Citation/Reference
X	Statute	Law Enforcement Suicide Data Collection Act, codified at 34 U.S.C. § 50701
	Executive Order	
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this

information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

The LESDC includes information about suicides or attempted suicides committed by LEOs. Each law enforcement agency voluntarily reports information for its current and former officers who commit or attempt to commit suicide. The LESDC is designed to collect data points as established within the LESDCA.

The LESDCA establishes requirements for the Attorney General, through the FBI, to collect and report information on law enforcement suicides and attempted suicides. The data collection must include the following information about law enforcement suicides and attempted suicides:

- the circumstances and events that occurred before each suicide or attempted suicide;
- the general location of each suicide or attempted suicide;
- the demographic information of each law enforcement officer who commits or attempts suicide;
- the occupational category, including criminal investigator, corrections officer, line of duty officer, and 911 dispatch operator, of each law enforcement officer who commits or attempts suicide;
- the method used in each suicide or attempted suicide.

To meet these requirements, the LESDC collects information within five respective areas:

- Administrative data pertaining to the LEO;
- Personal data pertaining to the LEO;
- General data pertaining to the incident;
- Circumstances of the incident;
- Wellness policy and training information from the LEO's agency.

In addition to the data elements regarding a suicide or attempted suicide incident, the NCA on LEEP receives the following data about its users: user ID, first and last name, agency email address, agency telephone number, employer/agency name and ORI, type of agency (e.g. federal, tribal), and user role.

The chart below outlines the information collected as part as the LESDC, as well as the user information collected by the NCA.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, and D	This applies to NCA users only; the LESDC does not collect the name of LEOs who commit or attempt to commit suicide.
Date of birth or age	X	A, B, C, and D	Date of birth is not collected; however, the LESDC collects the age of the LEOs who commit or attempt to commit suicide.
Place of birth			
Gender	X	A, B, C, and D	This applies to LEOs who commit or attempt to commit suicide.
Race, ethnicity or citizenship	X	A, B, C, and D	This applies to LEOs who commit or attempt to commit suicide.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
Business e-mail address	X	A, B, C, and D	The NCA collects the work email addresses of its users.
Business phone number	X	A, B, C, and D	The NCA collects the work phone numbers of its users.
Medical records number			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Medical notes or other medical or health information	X	A, B, C, and D	The LESDC collects as yes/no response as to whether LEOs who commit or attempt to commit suicide reported or suffered from the following medical issues: post-traumatic stress disorder, depression, alcohol/drug abuse, physical illness impacting the ability to perform job duties, domestic violence, or chronic illness. The LESDC also collects a yes/no response as to whether the LEOs who commit or attempt to commit suicide exhibited any mental health warning signs.
Financial account information			
Applicant information			
Education records			
Military status or other information	X	A, B, C, and D	The LESDC collects a yes/no response as to whether the LEOs who attempt or commit suicide were/are military veterans.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Employment status, history, or similar information	X	A, B, C, and D	The LESDC collects the following work-related information about LEOs who commit or attempt to commit suicide: years of service as a LEO, position status (e.g. active, retired, suspended), occupational category (e.g. officer, corporal, deputy, corrections officer, 911 operator), and whether the LEO was on/off duty at the time of the suicide or attempt. For users, the NCA collects the user's employing agency name, ORI, and agency contact information.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C, and D	The LESDC collects yes/no responses as to whether the LEOs who commit or attempt to commit suicide were involved in any internal investigations, disciplinary proceedings, promotions, or transfers.
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, and D	The LESDC collects yes/no responses as to whether LEOs who commit or attempt to commit suicide were scheduled to stand trial for criminal offenses and whether a guilty verdict would preclude further LE service.
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, and D	The LESDC collects yes/no responses as to whether LEOs who commit or attempt to commit suicide were scheduled to stand trial for any civil matters.
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C, and D	The LESDC collects the location at which the suicide or attempted suicide occurred (city, county, state, country) as well as the type of location (e.g. commercial building, government building, park, residence).
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:	X	A, B, C, and D	NCA audit logs collect information about users' access to the system.
- **User ID**	X	A, B, C, and D	
- **User passwords/codes**			
- **IP address**	X	A, B, C, and D	
- **Date/time of access**	X	A, B, C, and D	
- **Queries run**	X	A, B, C, and D	
- **Content of files accessed/reviewed**	X	A, B, C, and D	Audit logs also track changes users make to incident submissions.
- **Contents of files**	X	A, B, C, and D	

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Other (please list the type of info and describe as completely as possible):	X	A, B, C, and D	The LESDC collects the agency incident or case number assigned to the suicide or attempted suicide investigation, whether the LEO had children, the LEO's marital status, and general information about wellness training and services available at the LEO's agency. Additionally, the NCA collects the user's type of agency (e.g. federal, tribal) and user role. Through the NCA, users may also receive messages regarding data submissions, such as error and reject messages, data quality messages, and other messages regarding agencies' data submission statuses. The NCA will also capture user feedback provided during usability testing of the LESDC form.

Prior to launching the LESDC, the FBI will pilot the LESDC questionnaire with law enforcement agencies which qualify to report information to the LESDC. The pilot will include cognitive interviews and usability testing. The cognitive interviews consist of telephone interviews with participants. FBI interviewers will lead pilot participants through each question of the questionnaire and then allow participants to provide answers to probative questions to elicit their feedback on the type of questions asked and how they are presented as well as whether law enforcement agencies would have the requested information. Through the cognitive interviews, the FBI will identify potentially confusing questions, determine if law enforcement agencies will have the type of information they are being asked to provide, and identify potential improvements to the flow of the questions and the clarity of instructions. Notes from the cognitive interviews will not be stored in the NCA. The FBI will maintain the cognitive interview notes on internal FBI systems. Access will be limited to FBI personnel supporting the LESDC. Cognitive interview notes will generally be

maintained for two years; however, the FBI UCR Program may opt to retain the pilot data longer if operationally needed to effectively monitor the launch of the LESDC.

During usability testing, pilot participants will complete the LESDC questionnaire within the NCA. After completing the questionnaire, participants will fill out an after-action survey on the participants' experience in accessing the system, how long it took to complete the questionnaire, and the process of saving and submitting the form to the FBI UCR Program. The after-action surveys will be maintained within the NCA; however, they are not part of the actual LESDC.

After completing evaluation and analysis of the pilot results, the FBI UCR Program will draft a pilot report detailing the feedback collected during the interviews and usability testing, and discussing identified areas for improvement of the LESDC. The report will not identify any individual pilot participants. The FBI will provide the pilot report to the Office of Management and Budget (OMB) to assist OMB in providing feedback to the FBI on the LESDC before the launch of the full LESDC. In accordance with the LESDCA, the FBI will also provide the pilot report to Congress and make it available to the public.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	X
Phone	X	Email			
Other (specify): Only user information is provided directly from the individual to whom it pertains. Suicide incident information is not obtained directly from the individual about whom the information pertains. Rather, data elements are obtained by law enforcement agencies and submitted to the FBI by law enforcement agencies. Prior to the launch of the LESDC, the FBI will solicit user feedback on the proposed questionnaire via telephone.					

Government sources:					
Within the Component	X	Other DOJ Components	X		
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify):					

Non-government sources:					
Members of the public		Public media, Internet		Private sector	
Commercial data brokers					
Other (specify):					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component			X	As discussed above, FBI personnel supporting the LESDC have access to all LESDC incident submissions and user information in the NCA.
DOJ Components			X	Authorized DOJ users of the NCA have direct access to their agency users' data and LESDC incident submissions in the NCA.
Federal entities			X	Authorized federal users of the NCA have direct access to their agency users' data and LESDC incident submissions in the NCA.
State, local, tribal gov't entities			X	Authorized state, local, tribal, and other government entity users of the NCA have direct access to their agency users' data and LESDC incident submissions in the NCA.
Public		X		As previously discussed, incident information collected by the LESDC will be used to create statistical reports and publications. Statistical data cleared for public release will be made public through publications on the CDE. Publications will be designed to limit the ability of the reader or user to link information back to a particular LEO. In addition, the final report from the LESDC pilot will be publicly available.
Counsel, parties, witnesses, and possibly courts or other				

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):	X			As required by the LESDCA, the FBI will provide an annual report to Congress on the LESDC. The FBI will also provide the final report from the LESDC pilot to OMB and Congress.

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

Incident information collected by the LESDC will be used to create statistical reports and publications to aid in preventing future law enforcement suicides and promoting the understanding of suicide in law enforcement. Statistical data cleared for public release will be made public through publications on the CDE. The statistical information published will use aggregated data from incident submissions to the LESDC that will limit the ability of the reader or user to link information back to a particular LEO. For example, for publication purposes, sensitive indicators that have a high probability of disclosing identity, such as law enforcement agency, sex, race, or ethnicity, could be removed or aggregated into larger categories to minimize the risk of identifying a specific officer. As set forth in the LESDCA, the FBI will be working with the Federal Committee on Statistical Methodology's Confidentiality and Data Access Committee to develop publication policies to manage the risk of identity disclosure based upon best practices identified by other federal statistical programs. Best practices may include using a "10-observation" threshold[7] to limit the risk of discovering the identity of a LEO committing or attempting suicide. As the data collection develops, the UCR Program will continue to consult with the FBI's Privacy and Civil Liberties Unit regarding the publication strategy.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of

[7] A "10-observation" threshold requires data aggregation primarily by geography to a point where the totals in any particular field or cell in a table or totals by geographic identifier do not fall below 10 observations.

Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

The LESDC consists of two types of information: user information of individuals submitting suicide incidents through the NCA, and suicide incident submissions regarding LEOs who commit or attempt to commit suicide.

User Information: To receive an NCA account, users must complete the "Account Request Page," which leverages data about its users from LEEP (user ID, first and last name, agency email address, agency telephone number, employer/agency name and ORI). In addition, users are required to provide the user's type of agency (e.g. federal, tribal) and requested user role. The NCA's Access Request Page includes a Privacy Act statement informing potential users of the purpose for collecting their information and how it will be used. The Privacy Act Statement is also linked at the bottom of the NCA webpage. In addition, when accessing the NCA all users specifically agree to a government system notice informing them that they have no reasonable expectation to privacy regarding their activities on a government system and that their use of the government system may be monitored, intercepted, searched, and/or seized.

Incident Information: Submission of incidents to the LESDC is voluntary. Discretion for submittal lies with the law enforcement unit/department involved. Similar to the Uniform Crime Reporting system, law enforcement units/departments may not notify LEOs involved in suicide incidents that the information is being submitted. However, this PIA provides notice to the law enforcement community that the FBI will collect information about LEOs who commit or attempt to commit suicide and how that information will be used. In addition, the Paperwork Reduction Act (PRA) gives OMB authority over the collection of certain information by federal agencies. Information collections proposed by the FBI UCR Program, such as the LESDC, are subject to OMB review and approval, as set forth by the PRA's Information Collection Review process. The process for renewing or requesting approval for the collection of information involves submitting formal 60- and 30-day notices to the Department of Justice to be posted on the Federal Register detailing the intention of the data collection and a summary of the involved collection. These notices provide transparency to the public concerning federal collections and provide the public with an avenue to provide comments to the FBI UCR Program on the involved collection. The FBI is currently working with OMB on fulfilling its requirements under the PRA for the LESDC. Both the 60-day and 30-day periods for public comment must be completed before final approval for an information collection can be granted.

The FBI provides notice to all individuals providing feedback and incident information during the LESDC pilot about the reason for the pilot and the purpose of collecting their responses. Participation in the pilot is voluntary. By participating in the pilot, individuals consent to the collection and use of their responses.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

The purpose of the LESDC is to collect statistical information regarding LEOs who commit or attempt to commit suicides to prevent future law enforcement suicides and to promote understanding of suicide in law enforcement. The submission of incidents to the LESDC is voluntary and discretion for submittal lies with the law enforcement agency. Similar to the UCR system, the LESDC does not notify the LEO involved in the suicide incident that the information is being submitted nor does it request their consent. Information on a suicide incident is submitted voluntarily by the law enforcement agency whose officer was involved in the incident. Although there is a risk that data elements collected by the LESDC may be linked with information from other sources to identify a LEO, the data collection is designed to produce a national picture of law enforcement suicides, not to identify a specific LEO involved in a suicide incident.

Individuals participating in the LESDC pilot (i.e. cognitive interviews and usability testing) do so voluntarily. During the pilot, individuals can choose not to participate or not to provide a response to a specific question.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Incident information in the LESDC does not directly identify individuals. Law enforcement agencies submitting incident information to the FBI are responsible for ensuring its accuracy.

NCA users and pilot participants may request access to their records by following the guidance provided on the FBI's website at *https://www.fbi.gov/services/records-management/foipa*. A request for access to a record from this system of records must be submitted in writing and comply with 28 CFR part 16. Individuals may mail, fax, or electronically submit a request, clearly marked "Privacy Act Access Request," to the FBI, ATTN: FOI/PA Request, Record/Information Dissemination Section, 200 Constitution Drive, Winchester, VA 22602-4693; facsimile: 540-868-4995/6/7; electronically: *https://www.fbi.gov/services/records-management/foipa/requesting-fbi-records*. The request should include a general description of the records sought, and must include the requester's full name, current address, and date and place of birth. The request must be signed and dated and either notarized or submitted under penalty of perjury. While no specific form is required, requesters may obtain a form (Form DOJ-361) for use in certification of identity, which can be located at the above link. In the initial request, the requester may also include any other identifying data that the requester may wish to furnish to assist the FBI in making a reasonable search. The request should include a return address for use by the FBI in responding; requesters are also encouraged to include a telephone number to facilitate FBI contacts related to processing the request. A determination of whether a record may be accessed will be made after a request is received.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** The LESDC is a report type within the NCA. The NCA operates under the ATO for the UCR System. The UCR System was granted an ATO on December 14, 2018. The ATO currently expires on January 20, 2022. **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** All the security controls relevant to the UCR System and the NCA using National Institute of Standards and Technology (NIST) SP 800-37 and FBI OCIO policies have been reviewed and are continuously monitored in RiskVision.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The UCR system underwent a detailed evaluation in December 2018 and in June 2020. All identified critical and high vulnerabilities have been removed or mitigated. Other vulnerabilities have been mitigated or placed on the POAM worksheet for further evaluation for removal or mitigation. ISSOs conduct continuous evaluations and update the POAM report monthly. Quarterly, the report is formally presented to the stakeholders.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** Audit logs are retained for a minimum of one year, and security personnel review audit logs using automated log aggregation toolsets. SSAs monitor audit logs on a daily basis. The ISSO reviews audit logs, at a minimum, every seven days.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** For user reference, user guides and answers to frequently asked questions for both the NCA and the LESDCA are available within the NCA.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII

in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

The NCA is the collection platform for the LESDC and therefore controls the administrative, technical, and physical security for the data collection. UCR Operations, ISSOs, and the SSAs continually review the security controls for the NCA per the *FBI Security Assessment and Authorization Policy Guide* and also use the NIST Special Publication 800-53, for expanded definition and guidance. The ISSO is required to review security controls annually. This includes security controls focused on assessing risk to reduce the risk of unauthorized access, use, and disclosure. The risk assessment is reviewed and updated at least annually. The security impact level for confidentiality in the UCR system is moderate, and confidentiality is protected through acceptable security controls addressing boundary protection/external telecommunication, transmission confidentiality and integrity, and remote access/protection of confidentiality and integrity using encryption. The UCR inherits some security controls from both the FBI's CJIS Shared Enterprise Network and Data Center entities.

Contributing agencies can access the NCA via LEEP. The risk of unauthorized access or misuse of information in the NCA is mitigated by the use of two-factor authentication to log into LEEP. The information/data is further protected by role-based controls and access control list(s) at the group and individual level. Access to user information is restricted to the user, other users in the user's agency, other users in the user's chain of review, and FBI personnel supporting the NCA. User access to information within the NCA is strictly controlled to protect privacy and reduce the risk of unauthorized access and disclosure. System access is configured to ensure only personnel with the correct credentials may access data within the NCA. If an individual does not have specific access permissions to a particular piece of data, the individual will not be able to view that data. The NCA contains audit functions that can be used to detect improper use and/or access. All user and administrator actions are logged. SSAs monitor audit logs on a daily basis. The ISSO reviews audit logs, at a minimum, every seven days. Anomalous behavior or misuse of the NCA is subject to investigation and appropriate sanction, ranging from denial of access and elimination of privileges to referral to the FBI's Inspection Division, Internal Investigations Section, for investigation of FBI employee misconduct. Audit data from the NCA is supplied to the FBI's Enterprise Security Operations Center, which has a centralized view that can correlate audit information from different FBI systems.

All individuals with access to the NCA must comply with applicable security and privacy protocols address in the *CJIS Security Policy* (available at http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view), the *CJIS User Agreement*, and the *LEEP Rules of Behavior*. NCA users acknowledge that they understand sanctions may be applied for intentional misuse of the UCR system. General users must be knowledgeable of the *General User Security Guide (GUG)* and the privileged user must be knowledgeable of the *Privileged User Security Guide (PUG)*.

The NCA uses the AWS Gov-Cloud environment. Access to FBI information in the cloud infrastructure is limited to FBI personnel. Access by FBI personnel to specific FBI applications and datasets are determined at the application and dataset level. Both the FBI and AWS collect and maintain audit logs and user login identifiers; however, AWS personnel cannot access FBI applications or datasets, or the audit user activity therein. Data in transit is encrypted using Transport Layer Security Federal Information Processing Standard 140-2 encryption, and all interconnections

between the AWS Gov-Cloud and the FBI use firewalls and security filtering. The NCA is separated logically from other applications and is located in a private section of AWS Gov-Cloud managed by the FBI.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

The FBI's Information Management Division is currently developing a record retention schedule for the LESDC and any related publications. The data collected by the pilot testing will be maintained by the FBI for a minimum of two years after formal launch of the collection to all participating agencies, in keeping with typical record retention policies. The FBI UCR Program may opt to retain the pilot data longer if operationally needed to effectively monitor the launch of the LESDC.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X___ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

Audit logs are covered by *DOJ Computer Systems Activity and Access Records*, **DOJ-002**, 64 Fed. Reg. 73585 (Dec. 30, 1999), as amended at 66 Fed. Reg. 8425 (Jan. 31, 2001) and 82 Fed. Reg. 24147 (May 25, 2017).

NCA user information is covered by *Bureau Mailing Lists*, **JUSTICE/FBI-003**, 70 Fed. Reg. 7513 (Feb. 14, 2005), as amended at 82 Fed. Reg. 24147 (May 25, 2017); and *FBI Online Collaboration Systems*, **JUSTICE/FBI-004**, 82 Fed. Reg. 57291 (Dec. 2, 2017).

Incident data submitted to the LESDC does not create a system of records because none of the data elements in the LESDC directly identify an individual. Consequently, incident submissions cannot be retrieved by personal identifier of the LEO involved in the incident.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation

measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

The greatest privacy vulnerability created by the LESDC exists in the linkability of information collected with outside sources of information to potentially identify the LEO involved in a specific suicide incident. For example, if a suicide incident involves a female officer in a jurisdiction that has only one female officer, one would quickly be able to deduce the name of the officer involved. To limit the linkability of the data to specific LEOs, information regarding individual incidents will only be accessible to the submitters of that data, individuals in the submitter's chain of review, and FBI personnel supporting the LESDC. FBI publications will use aggregated data from incident submissions to the LESDC that will limit the ability of the reader or user to link information back to a particular individual. For example, for publication purposes, sensitive indicators that have a high probability of disclosing identity, such as law enforcement agency, sex, race, or ethnicity, could be removed or aggregated into larger categories to minimize the risk of identifying a specific officer.

To further mitigate the linkability risk to the extent possible, the LESDC collects only those data elements necessary to provide law enforcement and the nation with a comprehensive picture law enforcement suicide. To assist in developing the LESDC, the FBI created a task force made up of members of the LE community, including representatives from the International Association of Chiefs of Police, the National Sheriffs' Association, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), Major Cities Chiefs Association, and tribal LE representatives. The task force also includes representatives from the Bureau of Justice Statistics, academic experts in the fields of criminal justice and statistics, and subject matter experts on mental health and suicide events. Additional task force members are added as needed to ensure all types of LESDC participants are included (e.g. public safety telecommunicators, prosecutors). In determining which data elements to collect, the task force balanced the need to collect enough information to promote an understanding of law enforcement suicides with the privacy concerns in making the information linkable to specific individuals. For example, the task force decided not to collect the name of the LEO who commits or attempts to commit suicide because the personal identifier is not necessary to fulfill the purpose of the data collection.

As the LESDC evolves, the needs of the law enforcement community will determine any changes to the collected data elements. In addition to working with the LESDC task force, the FBI routinely works with federal, state, local, and tribal law enforcement representatives to decide which data elements are most beneficial by forming focus groups to discuss issues, trends, and changes needed to data collections. The FBI also receives recommendations from the Advisory Policy Board (APB)[8] and guidance from OMB to ensure the program only collects the minimum amount of

[8] The CJIS APB is a Federal Advisory Committee Act board comprised of state and local criminal justice agencies;

information needed.

There is an additional risk that information provided to the LESDC may not accurately portray the circumstances surrounding a law enforcement suicide. To ensure that publications from the LESDC are accurate and complete, the FBI relies on submitting agencies to indicate when the incident submissions are available for review and use. To assist agencies in submitting complete and accurate information, the LESDC report form includes business rule logic. The logic is intended to guide the submitter through the application based on elements applicable for the incident. Submitter responses will indicate the mandatory fields based on the reasonable responses to the incident details. The LESDC report form also includes general "tool tip" capabilities which provide additional context to the questions and ensure users understand the intent of the question and the possible response selections. Once the agency representative is satisfied that the incident information is complete and ready for publication use, the agency representative will approve the incident for further use. Other users in the submitter's chain of review will also have the opportunity to review incident information for completeness and quality. The FBI's publications will only use incident information that has been approved for further use by the submitting agency.

As discussed in section 3.1, the FBI will begin the LESDC as a pilot. The pilot will allow the FBI to determine if submitting agencies understand the intent behind the questions in the LESDC and the workflow of the report form. At the end of the pilot, the FBI will analyze the data collected during the pilot phase to determine if users are understanding the questions and submitting appropriate responses. The FBI will compile a final report on the result of the pilot and provide the report to OMB and Congress. The report will also be available to the public. The pilot report will not identify any specific pilot participants. The results of the pilot may result in changes to the LESDC.

The only directly identifiable information contained within the LESDC is the user information collected by the NCA. User information is limited to information necessary to communicate with users and ensure their authorization to submit data to the UCR Program. Access to a specific user's information in the NCA is role-based and restricted to the user, other users in the user's chain of review, and FBI personnel supporting the NCA, including system and database administrators. Any privacy risks associated with the collection of system user information are outweighed by the necessity that the national UCR Program be able to communicate and collaborate with its data submitters.

---

members of the judicial, prosecutorial, and correctional segments of the criminal justice community; representatives of federal agencies participating in the CJIS systems; and representatives of criminal justice professional associations. The purpose of the APB is to recommend to the FBI Director general policy with respect to the philosophy, concept, and operational principles of various criminal justice information systems managed by the FBI's CJIS Division.