Federal Bureau of Investigation

Privacy Impact Assessment
for the
Law Enforcement Officers Killed and Assaulted (LEOKA)
Data Collection

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

Approved by: Jay Sinha
Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: May 5, 2025

(May 2022 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.)

The Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division's Uniform Crime Reporting (UCR) Program is a collective effort by federal, state, local, tribal, and territorial law enforcement agencies to present a nationwide view of crime. The FBI UCR Program includes the Law Enforcement Officers Killed and Assaulted (LEOKA) Data Collection. The LEOKA Data Collection also is a collective effort by federal, state, local, tribal, and other types of law enforcement agencies to present a nationwide view of data in reference to law enforcement officers killed and assaulted in the line of duty. Recently, the data collection expanded to include the collection of law enforcement health-related deaths. The main purpose of the LEOKA Data Collection is to perform detailed analyses on incidents in which law enforcement officers are killed or assaulted in the line of duty while enforcing laws and maintaining public order, or who die from health-related incidents directly related to performing their duties as a sworn law enforcement officer.

The LEOKA Data Collection collects details regarding line-of-duty deaths and assaults occurring nationwide and shares that national picture with the law enforcement community in the hopes of preventing further line-of-duty deaths and assaults. The FBI UCR Program is modifying the platforms through which it collects and manages LEOKA data and automating the collection of LEOKA data to provide more complete data for analyses and to reduce the burden for data contributors. The FBI UCR Program recently began collecting LEOKA assault data exclusively via the National Incident-Based Reporting System (NIBRS)[1] and uses an electronic reporting form within the Collection of Law Enforcement and Crime Tool (COLECT)[2] to gather information about LEOKA health-related deaths. The FBI UCR Program's new LEOKA application will provide electronic data collection forms and consolidate LEOKA data for more efficient and secure collection, management, and release. This Privacy Impact Assessment (PIA) addresses the privacy issues associated with the collection and release of information about officers, circumstances, and offenders involved in LEOKA incidents and users of the LEOKA application.

---

[1] The PIA for the UCR System addresses NIBRS: https://www.fbi.gov/file-repository/pia-uniform-crime-reporting-system-020823.pdf/view.

[2] COLECT is a web-based application that enables federal, state, local, tribal, and territorial agencies to submit information to the FBI UCR Program for multiple data collections, in this case, LEOKA health-related deaths. COLECT has separate privacy documentation: https://www.fbi.gov/file-repository/pia-collection-of-law-enforcement-and-crime-tool-110822.pdf/view.

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.

The LEOKA Data Collection is a collective effort by federal, state, local, tribal, and other types of law enforcement agencies to present a nationwide view of data about law enforcement officers killed and assaulted in the line of duty. This data collection's main purpose is to perform detailed analyses on incidents in which law enforcement officers are feloniously or accidentally killed or who are assaulted in the line of duty while enforcing laws and maintaining public order. In 2020, the FBI's UCR Program began collecting information about officer deaths resulting from duty-related health conditions. Information about health-related deaths include counts of deaths from SARS-COVID-19, heart attacks, and deaths resulting from responding to the events of 9/11/2001. Information about the LEOKA Data Collection is available online at fbi.gov.

The LEOKA Data Collection seeks to reduce incidents of law enforcement officer deaths and assaults against them and raise awareness of these tragedies by providing data for research and instructional services about law enforcement safety. The collection of LEOKA data provides information for statistical data releases through the FBI's UCR Program and the delivery of Officer Safety Awareness Training (OSAT) nationwide. It also benefits law enforcement agencies in several ways. Representatives within law enforcement agencies use the data to design new policies or modify existing ones, determine resources needed by the officers or if additional personnel are required, and develop officer safety training specific to their agency.

The FBI CJIS Division uses LEOKA data to develop OSAT, which FBI CJIS Division personnel provide to law enforcement agencies across the country, and to conduct in-depth research on the circumstances surrounding assaults and killings of law enforcement officers. The FBI UCR Program further uses the collected information to provide a public view of law enforcement officers killed and assaulted through its statistical publications and summary infographics available online via the UCR Crime Data Explorer (CDE).[3]

The FBI collects LEOKA data via reporting forms hosted on the Law Enforcement Enterprise Portal (LEEP).[4] Felonious killings and accidental deaths are collected with electronic versions of the 1-701 and 1-701a forms.[5] To facilitate easier submission of felonious and accidental death data, the FBI is redesigning its LEOKA application to allow authorized LEOKA data contributors to directly input and manage their LEOKA felonious and accidental death information.

---

[3] The UCR System PIA addresses the CDE.
[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 and ensuring only authenticated users have access to those systems and services. LEEP has separate privacy documentation.
[5] LEOKA's data collection is subject to the Paperwork Reduction Act and therefore undergoes Office of Management and Budget (OMB) review and approval. OMB No. 1110-0009.

The FBI LEOKA staff input health-related death information via a reporting form (Law Enforcement Health Related) on COLECT. Agencies submit LEOKA assault data through NIBRS, which is submitted via COLECT or electronic file submissions. To provide a comprehensive data set for LEOKA incidents, the LEOKA application ingests the health-related death information from COLECT every 30 days and ingests the LEOKA assault data from NIBRS every 30 days. LEOKA staff use all the information in the LEOKA application to provide a comprehensive view of incidents and circumstances, officers, and offenders (where applicable); enable data analyses; and streamline publications.

To access the LEOKA application, authorized LEOKA data contributors log in to LEEP and choose the LEOKA icon. Authorized LEOKA data contributors include personnel from federal, state, local, college/university, tribal, and territorial law enforcement agencies. Once logged in to the LEOKA application, authorized LEOKA data contributors can enter, save, review, and submit LEOKA line-of-duty deaths to the LEOKA Data Collection.

The FBI UCR Program recently began gathering LEOKA assault data via NIBRS and documenting health-related deaths through a reporting form on COLECT. Law enforcement health-related information is gathered from the FBI's Strategic Information and Operations Center (SIOC) and notifications from the Officer Down Memorial Page (ODMP). The LEOKA staff enter the data into the Law Enforcement Health Related (LEHR) form on COLECT. Assaults and health-related deaths are used for counts only, and no personally identifiable information (PII) about the officers is collected.

The FBI's UCR Program LEOKA staff use line-of-duty death notifications received from SIOC, the ODMP, and open-source data collected by FBI CJIS Division staff to initiate an incident entry within the LEOKA application. LEOKA staff then reach out to the affected agencies to assist them in providing the requested LEOKA incident details. Affected agencies verify the initial information and provide additional information about the LEOKA incidents. The LEOKA application is designed to minimize the use of separate Microsoft Excel spreadsheets, Microsoft Word documents, and computer files and facilitate data analyses for publications and OSAT research and training. The LEOKA application uses role-based access controls to secure and protect data while permitting its use when necessary and permissible. FBI CJIS Division staff (OSAT and Statisticians) have access to the LEOKA application to view data that may facilitate research and analysis. (See Section 4.1 for information about user roles). A monthly infographic provides preliminary and confirmed counts on felonious killings, accidental deaths, and health-related deaths gathered from all collection sources. The annual LEOKA data release incorporates preliminary and agency confirmed information.

In addition to using LEOKA data to provide statistics about officers killed, assaulted, and health-related deaths, the FBI uses LEOKA incident information for in-depth research studies approved by the FBI's Institutional Review Board (IRB).[6] For example, FBI staff may search the

[6] The IRB is a review committee established to help protect the rights and welfare of human research subjects. The FBI's IRB is required to review and approve/disapprove any research sponsored or supported by the FBI that involves or affects, directly or indirectly, human subjects. The core function of the IRB is to ensure the protection of the health, safety, well-being and legal rights of humans who are the subjects of research sponsored by the FBI. The FBI's IRB is governed by federal regulations which can be found beginning at 28 C.F.R. § 46.101.

LEOKA data to identify all cases within a 10-year period that involved the victim officer being feloniously killed in ambush-style attacks. FBI staff then review the incidents. After identifying sample cases, FBI OSAT staff contact the officers and offenders involved in the incident and ask for their consent to participate in the research study. With each participant's consent, the FBI administers questionnaires and conducts interviews regarding the incident. With consent, the interview may be recorded, transcribed, and used for research and training purposes. Once the research information is gathered, FBI OSAT staff work with approved research partners to analyze the data and create reports and OSAT. Information gathered through LEOKA research is maintained separately from the LEOKA incident data in the LEOKA application.

Finally, the FBI compares offender data from LEOKA incidents to other FBI data. For example, the National Crime Information Center (NCIC) Program and UCR Program worked collectively to determine which offenders within the LEOKA data collection may qualify for entry into the NCIC Violent Person File (VPF).[7] The comparison led to increased collaboration between the NCIC Program Office and the UCR Program Office in discussions with the law enforcement community to emphasize the importance of leveraging NCIC's VPF to provide law enforcement nationwide with additional information on potentially violent individuals. Similar data comparisons may lead to other initiatives to improve the visibility of the LEOKA Data Collection and broaden understanding of how it can inform operational discussions to improve officer safety.

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
Statute	28 U.S.C. § 534 (a) and (c); 34 U.S.C. §§ 41303, 41311
Executive Order	
Federal regulation	28 CFR 0.85(f)
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	June 17, 1971, Memorandum to the Director of the FBI from the Executives of the Prevention of Police Killings Conference recommending that the FBI's UCR Program collect detailed data on law enforcement officers killed in the line of duty.

[7] NCIC's VPF contains records of individuals who have been convicted of violent crimes against law enforcement, have made credible threats of violence against a member of the law enforcement or criminal justice community, have been convicted of a violent crime against a person, or have been convicted of a violent crime where a firearm or weapon was used. The VPF was designed to alert law enforcement officers that an individual they are encountering may have the propensity for violence against law enforcement. For more information about NCIC, please see the NCIC PIA.

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.

As stated above, the LEOKA Data Collection collects information regarding incidents in which law enforcement officers are killed and assaulted in the line of duty, as well as health-related death information.

For felonious and accidental line-of-duty deaths, detailed LEOKA data contains information about the victim officer who was killed during the incident, details surrounding the incident, and information about the offender(s). Information about the victim officer includes the officer's name, date of birth (DOB), age, sex, race and ethnicity, height, weight, total law enforcement experience, and information about the officer's injuries. Information about the offender includes the offender's name, DOB, age, sex, race and ethnicity, height, weight, last know city of residence, Universal Control Number (UCN),[8] information about the offender's background with the criminal justice system, and information about the offender's injuries, if applicable.

For health-related deaths, the LEOKA Data Collection gathers the officer's agency and associated originating agency identifier (ORI), the officer's rank at the time of the officer's death, officer's age at time of death, the cause of death (COVID 19, 9/11-related, and other), and date of death. The LEOKA Data Collection does not collect the name of officers who pass away due to health-related injuries.

In addition to information about officers and offenders involved in LEOKA incidents, the LEOKA application collects and maintains information about its users. The LEOKA application collects information for individuals who are submitting data such as name, telephone number, and email address. The LEOKA application also maintains audit log information regarding users who access the database. This information includes usernames, federated identities, login date, and status (successful/failed login attempt). Further, the LEOKA application includes a record status history which shows the user who created an entry and the user who last modified an entry.

[8] The UCN, also known as the FBI Number, is a unique identification number assigned to each identity in the Next Generation Identification (NGI) system. The NGI system has separate privacy documentation.

The following chart visibly depicts the type of information collected by the LEOKA Data Collection and application.

(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	For LEOKA application users, offenders, and officers.
Date of birth or age	X	A, B, C, and D	LEOKA information includes the age and DOBs of the offenders and officers.
Place of birth			
Sex	X	A, B, C, and D	LEOKA collects the sex of the offenders and officers.
Race, ethnicity, or citizenship	X	A, B, C, and D	LEOKA collects the race and ethnicity of the offenders and officers.
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			
Work mailing address	X	A, B, C, and D	LEOKA collects the address for the officer's agency. For offenders, LEOKA collects only the offender's last known city of residence.
Work e-mail address	X	A, B, C, and D	The LEOKA application maintains email addresses for its users and data contributors; C and D apply to employees of non-federal agencies who may include non-USPER employees (still fully vetted for access to CJIS systems).
Work phone number	X	A, B, C, and D	The LEOKA application maintains the agency phone number for its users; C and D apply to employees of non-federal agencies who may include non-USPER employees (still fully vetted for access to CJIS systems).
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	LEOKA incidents contain information about injuries sustained by the involved officers and offenders and whether the offender was impaired at the time of the incident.
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information	X	A, B, C, and D	LEOKA collects the years (months/years) of service and rank of officers; C and D apply to officers of non-federal agencies who may include non-USPER employees.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C, and D	LEOKA collects officers' years of service and whether they had specific training; C and D apply to officers of non-federal agencies who may include non-USPER employees.
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C and D	LEOKA collects the UCN of the offenders and information about their background with the criminal justice system (e.g., history of types of offenses, probationary status). For felonious killings, LEOKA also collects whether the offender was listed in the NCIC VPF.
Juvenile criminal records information	X	C and D	LEOKA collects the UCN of the offenders and information about their background with the criminal justice system (e.g., history of types of offenses, probationary status), which may include juvenile criminal history information.
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			

(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
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 LEOKA application collects incident location details as NIBRS location codes (e.g., business, residence, park).
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**	X	A, B, C, and D	Offenders and officers may consent to being video recorded for IRB-approved research studies. The video recordings are not stored in the LEOKA application. In addition, the FBI may obtain dashboard camera or body camera footage as part of IRB approved research studies into LEOKA incidents. This video footage is not stored in the LEOKA application.
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**	X	A, B, C, and D	Offenders and officers may consent to being video recorded for IRB approved research studies. The video recordings are not stored in the LEOKA application. In addition, the FBI may obtain dashboard camera or body camera footage as part of IRB-approved research studies into LEOKA incidents. This video footage is not stored in the LEOKA application.
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			

(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
System admin/audit data:	X	A, B, C, and D	The LEOKA application and COLECT audit logs capture information about users accessing the system; C and D apply to employees of non-federal agencies who may include non-USPER employees (still fully vetted for access to CJIS systems).
- **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	The LEOKA application and COLECT audit logs also track changes users make to incident submissions.
Other (please list the type of info and describe as completely as possible):			LEOKA incident submissions also include details surrounding the line-of-duty death, such as location, date/time, circumstances, weather conditions, location of injuries, type of weapons, body armor usage, number of rounds fired, etc. In addition, the LEOKA incident submissions will include the corresponding NIBRS incident number (if applicable) and the National Use-of-Force Data Collection case number (if applicable).

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	X	Hard copy: mail/fax		Online	X
Phone	X	Email	X		
Other (specify): LEOKA application users directly provide their information to the FBI's UCR Program online. Law enforcement agencies provide LEOKA incident submissions. After submission, if an incident is selected to be part of a research study, additional information about the incident may be provided directly from the officer and/or offender involved in the study. Contributing law enforcement agencies will submit LEOKA data to the FBI online via the LEOKA application or NIBRS (for assault information). LEOKA staff submit health-related deaths via COLECT.					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	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	X	Private sector	
Commercial data brokers					
Other (specify): Preliminary LEOKA data is captured from public websites and used for daily communications to leadership, monthly infographic counts, and publications/data releases. Incident details are verified with the officers' agencies. Open-source data also provides data quality to ensure incidents known to law enforcement are submitted to the LEOKA Data Collection by the officers' agencies.					

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		X	FBI personnel supporting the LEOKA Program have direct access via LEEP to the LEOKA application dependent on user role access for information submitted to LEOKA, Sentinel, [9] and COLECT. Within the LEOKA application, FBI field office personnel submitting LEOKA incidents have access to their incidents.
DOJ Components			X	Users with LEOKA application accounts have direct log-in access via LEEP to LEOKA information submitted by their assigned ORIs.
Federal entities			X	
State, local, tribal gov't entities			X	
Public		X		The FBI will publish preliminary counts, aggregated statistical data, and case summaries of LEOKA information on the CDE.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				

[9] Sentinel is the FBI's case management system. Sentinel is covered by separate privacy documentation.

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.**
Other (specify):	X	X		Upon request, the LEOKA Program may provide incident-level data to individuals/entities for research or other purposes. All directly identifying information is removed from incident-level data before it is released.

The submission method for LEOKA information controls access to the submitted data. COLECT controls access to LEOKA health-related death incidents; NIBRS controls access to LEOKA assault data, and the LEOKA application controls access to LEOKA felonious and accidental death incidents. Access to all LEOKA incident data is limited to authorized data submitters. Authorized LEOKA data submitters include personnel from federal, state, local, college/university, tribal, and territorial law enforcement agencies with the ability to contribute data to the LEOKA Data Collection. Agencies must have a UCR-recognized ORI to contribute LEOKA data.

Agency users with a valid UCR ORI can apply for account access to the LEOKA application via LEEP by submitting an access request. Once approved for access, users are assigned a user role that controls their ability to view, enter, and manage data within the LEOKA application. Users assigned the Submitter role can update incidents on behalf of their agency, indicate whether their incident is complete, and submit the incident to the FBI's UCR Program on behalf of their agency. LEOKA Submitters can also view the incident transaction history for incidents associated with their assigned ORIs.

The FBI UCR Program controls initial LEOKA application account access for agencies. Once the FBI UCR Program establishes an agency point of contact (POC) in the LEOKA application, the POC is assigned a Submitter role and the appropriate ORIs associated with the user's area of responsibility. FBI Administrators can create, approve, update, assign, and delete roles and privileges for LEOKA application users. FBI personnel supporting the LEOKA Data Collection in the FBI Administrators role control which users can view, modify, submit, download, and export LEOKA information. These FBI Administrators also have the functionality assigned to the Submitter role and can view the transaction history for any incidents to assist users in entering, managing, validating, or updating their data. FBI Administrators can view all entries within the LEOKA application; create data for training purposes and take data through the workflow process (completion, review, data quality checks, and submission); create an incident on behalf of a requesting agency; indicate whether an incident is complete and submit an incident on behalf of a requesting agency; inform data owners if the data needs to be updated; query data; view dashboards; export data to spreadsheets; and view the transaction history for LEOKA incidents. All finalized incident submissions are also stored in Sentinel. FBI personnel supporting the LEOKA Data Collection can also access LEOKA health-

related incident information within COLECT.[10]

FBI System Administrators are responsible for maintaining the LEOKA application and can view and access the LEOKA application data. FBI System Administrators are responsible for maintaining the software, security, and hardware and also have the same functionality as the FBI Administrator role.

FBI OSAT personnel are assigned read-only access to view incidents that contain PII within the LEOKA application, which can inform OSAT activities, including research and training development.

The FBI also may use LEOKA information to develop OSAT materials and provide OSAT to law enforcement agencies. Raw materials collected during research, including videos and transcripts of interviews with officers and offenders, are available only to FBI personnel and FBI research partners who have been approved by the FBI's IRB. The FBI's IRB reviews and approves all research projects and partners. Any entities partnering with the FBI for research purposes are required to sign an information transfer agreement requiring them to maintain the confidentiality of any information provided for research, outlining safeguard procedures for storing the information, limiting the use of the data provided, and setting forth the destruction requirements once the research project is complete. Information the FBI obtains pursuant to research activities (e.g., videotaped interviews, protocol questionnaires) is accessible only to the FBI staff and research partners involved in the research who have signed data transfer agreements. Information derived from the research is used to create training materials for the FBI's OSAT courses. With the offenders' and officers' consent, trainers may use portions of videotaped interviews for OSAT. The FBI may also use research information to publish information on specific topic areas pertinent to officer safety, such as ambushes and unprovoked attacks. Publications do not include officers' or offenders' names or other directly identifying information.

Additionally, local, state, tribal, federal, and international law enforcement agencies may request statistical LEOKA information, without officers' or offenders' names, to perform their own research on specific topics of interest, (e.g., use of body armor, weapon information, etc.).

When submitting a LEOKA feloniously killed incident via the LEOKA application, submitting agencies may choose to have the offender entered into the NCIC's VPF if the offender meets the entry criteria for the VPF. If the agency requests the FBI to enter the offender into the VPF, the UCR Program will extract relevant data from the LEOKA incident and provide it to the NCIC Program for entry into the VPF. Although the FBI would create the initial entry at the agency's request, the agency will be responsible for all subsequent record maintenance such as validation requirements, providing additional information about the offender, and maintaining documentation to support the entry of the individual's information in the VPF.

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

[10] FBI personnel supporting the LEOKA Program also have access to LEOKA assault data submitted via NIBRS. Access to NIBRS data, including collected LEOKA assault data, is discussed in the UCR System PIA.

research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

The FBI releases statistical LEOKA data and incident summaries cleared for public release through publications on fbi.gov or the CDE. Publicly released information does not include directly identifying information. Before release, the FBI typically redacts names, DOBs, addresses, agency incident or case numbers, offender's FBI number, and offender's date of arrest. Case summaries for felonious incidents are provided by the contributing law enforcement agency. The summaries are reviewed and frequently redacted before public dissemination.

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 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 purpose of the LEOKA Data Collection is to collect information regarding law enforcement line-of-duty assaults and deaths, to use this information to provide an aggregated view of such incidents, and to develop OSAT. The submission of LEOKA incidents is voluntary, and discretion for submittal lies with the involved officer's law enforcement agency. Because LEOKA information is submitted by the law enforcement agency, and not directly by the officer or offender involved, the FBI does not provide any direct notice to the officer or offender that their information is being submitted to the LEOKA Program.

If the FBI chooses an incident as part of an in-depth research study and makes direct contact with the involved officer or offender, the FBI explains the goal of the study and how provided information (including recorded interviews and responses) will be used. Officers and offenders participating in LEOKA research projects provide specific consent to be interviewed, recorded, and allowing the FBI to use their information for OSAT purposes.

Individuals applying for access to the LEOKA application receive a Privacy Act notice informing them about why their information is being collected and how it will be used.

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.

Law enforcement agencies generally do not request the consent of the individuals involved in the incident (law enforcement or civilian) before submission and do not notify or request consent for utilization of this data. The LEOKA Data Collection is a voluntary program. Law enforcement agencies are not required to submit data.

Officers and offenders participating in LEOKA research projects provide specific consent to be interviewed, recorded, and allowing the FBI to use their information for OSAT purposes. They can discontinue their participation in the research study at any time.

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.

Individuals may request access to their records by following the guidance provided on the FBI's website. A request for access to a record from this system of records must be submitted in writing and comply with 28 CFR part 16. 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).

This section pertains specifically to the LEOKA application. For information about the security of COLECT and NIBRS, please see the privacy impact assessments for COLECT and the UCR System, available on fbi.gov.

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 LEOKA application currently operates under the ATO for the National Use-of-Force Data Collection (NUOFDC) . The NUOFDC ATO expires on 11/20/2025. **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 moderate security controls relevant to the NUOFDC system using NIST Special Publication (SP) 800-53 and FBI Office of Chief Information Officer policies have been reviewed and are continuously monitored in JCAM. Information System Security Officers (ISSOs) conduct continuous evaluations, and monthly status reports are presented to the Assistant Section Chief of the Information Technology Management Section.
	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	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and**

	consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan: The NUOFDC, including the LEOKA application, was evaluated for FIPS 199 categorization and was assigned categories of moderate confidentiality, low integrity, and low availability. The moderate confidentiality level is based on the limited adverse effect on agency operations, agency assets, or individuals for the unauthorized disclosure of information, including the minimal PII in the system. The low integrity level is based on unauthorized modification or destruction of information potentially adversely affecting operations or public confidence in the agency, but the damage to the mission would usually be limited. The low availability level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to the information. Mission use of this dataset may be tolerant of delay in re-establishing access to the information.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The NUOFDC System underwent evaluation in November 2022. All vulnerabilities have been mitigated or placed on the Plan of Action and Milestones worksheet for further evaluation for removal or mitigation. ISSOs conduct continuous evaluations, and monthly status reports which are available for the system owner.
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 track system and database administrator access of information. Tripwire monitors system file access for changes. The information system logs user access and tracks changes made to NUOFDC incident submissions. System Security Administrators (SSAs) monitor audit logs on a daily basis. The ISSO reviews audit logs, at a minimum, every seven days. Security personnel review audit logs using automated log aggregation toolsets.
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 are available within the LEOKA application.

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?

LEOKA incidents are submitted via the LEOKA application, which controls the security for the submitted information. The NUOFDC Operation Team, ISSOs, and the SSAs continually review the security controls for the LEOKA application per FBI policy and use 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. 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 LEOKA application inherits some security controls from both the FBI's CJIS Shared Enterprise Network and Data Center entities.

Users access the LEOKA application via LEEP. LEEP mitigates the risk of unauthorized access by requiring multi-factor authentication for log in. LEEP is a federated gateway that securely connects law enforcement, criminal justice, and homeland security communities to applications and services over the Internet. LEEP provides users with access to the LEOKA application while still maintaining the constraints of the *CJIS Security Policy* and the FBI's Rules of Behavior for General Users. Access to LEEP is gained through an Identity Provider (IdP). 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 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 the user to access Service Providers, in this case the LEOKA application. When a user selects the LEOKA application icon, LEEP passes the users attributes to the LEOKA application for authentication. Once logged in to the LEOKA application, the system determines which information within the system the users can access. Access is determined based on the user's attributes and assigned roles as outlined in Section 4.1.

The information/data is further protected by role-based controls and access control list(s) at the group and individual level. User access to information within the LEOKA application 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 LEOKA application. 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 LEOKA application contains audit functions used to detect improper use and/or access. The LEOKA application logs all user and administrator actions. SSAs monitor audit logs daily. The ISSO reviews audit logs, at a minimum, every seven days. Anomalous behavior or misuse of the LEOKA application 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 LEOKA application 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 LEOKA application must comply with applicable security and privacy protocols addressed in the *CJIS Security Policy*, the *CJIS User Agreement*, and the *LEEP Rules of Behavior*. LEOKA application users acknowledge that they understand sanctions may be applied for intentional misuse of the system. General users must be knowledgeable of the security practices for general users and the privileged user must be knowledgeable of the security practices for privileged users.

The LEOKA application utilizes the FedRAMP certified Amazon Web Services (AWS) Government-Cloud (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. The FBI collects and maintains audit logs and user login identifiers. AWS personnel cannot access FBI applications or datasets or 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 NUOFDC 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.)

Incident submissions to LEOKA will be retained permanently as set forth in the approved National Archives and Records Administration (NARA) schedule, NARA Job Number N1-065-07-22. Publications from the LEOKA submissions will be retained permanently. The LEOKA application maintains audit logs for two years.

LEOKA research materials such as videos, transcripts, and aggregated data are used to create OSAT materials. Some videos of interviews conducted during the research are edited and become part of the OSAT curriculum. In accordance with NARA Job Number N1-065-07-04, those videos and training materials will be retained for twenty-five years after the completion of the OSAT program.

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:

FBI Online Collaboration Systems, **JUSTICE/FBI-004**, 82 FR 57291 (Dec. 4, 2017), available at https://www.govinfo.gov/content/pkg/FR-2017-12-04/pdf/2017-25994.pdf.

The FBI Central Records System, **JUSTICE/FBI-002,** 63 FR 8659, 671 (Feb. 20, 1998) as amended by 66 FR 8425 (Jan. 31, 2001), 66 FR 17200 (Mar. 29, 2001), and 82 FR 24147 (May 25, 2017), available at https://www.justice.gov/opcl/doj-systems-records#FBI.

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.***

As discussed above, LEOKA incident information is collected from the victim officer's law enforcement agency and generally not directly from the victim officer or offender. Because the information is not collected directly from individuals involved in the incident, there is a risk that the information may be inaccurate. However, LEOKA staff check the submitted data for inconsistencies by comparing the data provided by the submitter and the incident details included in the submitted incident summary. The LEOKA application's design also assists users in completing all necessary information by notifying users of incomplete data fields before submitting their incident details. A submitter can review historical incidents entered in the new application and communicate with LEOKA staff for potential concerns or questions. Information collected from other sources may augment agency reports preliminarily, including health-related deaths. When LEOKA staff identify incomplete items or inconsistencies in the data, they request further clarification from the submitting agency. In addition, if an incident is selected as part of a research study, additional information about the incident may be gathered directly from the officer and/or offender involved which helps ensure the accuracy of information used for research studies.

To further mitigate privacy risks, the FBI collects only the minimum amount of information needed to provide a comprehensive view of LEOKA incidents. Information collected by the LEOKA Data Collection has been determined throughout the years by the needs of the law enforcement community. The FBI routinely works with local, state, tribal, and federal law enforcement representatives to decide which data elements are most beneficial by forming focus groups to discuss issues, trends, and changes in the behaviors of offenders. In addition to these focus groups, the FBI also receives recommendations from the CJIS Advisory Policy Board (APB)[11] and guidance from OMB to ensure the program only collects the minimum amount of information needed. For example, in 2020, the FBI's UCR Program convened the Beyond 2021 LEOKA Task Force, comprised of representatives from federal, state, and local law enforcement agencies. The mission of this group was to assist the FBI's UCR Program with updating and modernizing the LEOKA Data Collection. Several recommendations from the task force were proposed to reduce the burden of the law enforcement agencies responsible for submitting LEOKA incident data. Through collaboration with the Beyond

[11] The CJIS APB is a Federal Advisory Committee Act board comprised of state and local criminal justice agencies; 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 APB makes recommendations to the FBI Director about general policy with respect to the philosophy, concept, and operational principles of various criminal justice information systems managed by the FBI's CJIS Division.

2021 LEOKA Task Force, the FBI's UCR Program modified the LEOKA Data Collection tools to ensure the data collected is relevant and effective for enhancing officer safety.

To further reduce risks to privacy associated with the collection of officers' and offenders' information, the LEOKA Data Collection limits the information it makes publicly available. Although the LEOKA Data Collection collects individuals' names and dates of birth, this collected PII is not publicly released. Rather, as discussed above, LEOKA data is published and released in an aggregated format. Similarly, detailed information collected during research, such as officer and offender interviews, is not publicly released. More detailed information collected during research is used to develop OSAT materials (which the FBI provides only to law enforcement representatives) and to create law enforcement publications that do not identify specific officers or offenders. OSAT materials are also available to law enforcement personnel and other authorized LEEP users via LEEP. The FBI obtains consent from officers and offenders before using any video clips during OSAT.