Federal Bureau of Investigation (FBI)

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

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

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

Date approved: [July 16, 2019]

(May 2015 DOJ PIA Form/FBI revision August 1, 2017)

EXECUTIVE SUMMARY

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, and tribal law enforcement agencies to present a nationwide view of crime. The FBI UCR Program includes the Law Enforcement Officers Killed and Assaulted (LEOKA) Program. The LEOKA Program 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. This data collection's main purpose 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. The LEOKA Program 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. CJIS is developing a new LEOKA database to automate the collection of LEOKA information from participating law enforcement agencies. This Privacy Impact Assessment addresses the privacy risks and mitigations regarding collecting personally identifiable information (PII) on officers and offenders and the sharing of such information.

Section 1: Description of the Information System

(a) The purpose that the records and/or system are designed to serve:

The LEOKA Program 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. This data collection's main purpose 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. The LEOKA Program 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. More information about the LEOKA Program is available online at <https://www.fbi.gov/services/cjis/ucr/leoka>.

(b) The way the system operates to achieve the purpose(s):

The LEOKA Program prevents further line-of-duty deaths and assaults on the nations' law enforcement officers through data collection, research, and instructional services. With the collected information, the LEOKA Program develops Officer Safety Awareness Training (OSAT), which LEOKA personnel provide to law enforcement agencies across the country. Additionally, the LEOKA Program uses the information in conjunction with interviews of officers and offenders to conduct in-depth research on the circumstances surrounding assaults and killings of law enforcement officers. The LEOKA Program further uses the collected information to provide a public view of law enforcement officers killed and assaulted through its annual statistical publication and summaries available at <https://ucr.fbi.gov/leoka-resources>. In the future, statistical information may also be available online

through the UCR Crime Data Explorer (CDE).[1]

Currently, the LEOKA Program receives information from participating law enforcement agencies through paper forms which are completed and electronically transmitted, emailed, mailed, or faxed to the LEOKA Program. The LEOKA Program personnel then manually enter information from the forms into a LEOKA database. CJIS is developing a new LEOKA database to automate the collection of LEOKA information from participating law enforcement agencies. The intent of the new LEOKA database effort is to meet user needs by:

- Creating a searchable data repository for internal FBI stakeholders;
- Establishing LEOKA interoperability between the FBI and law enforcement data contributors via the Law Enforcement Enterprise Portal (LEEP)[2] for user authentication and access. To facilitate authentication and access, LEEP collects the following information on LEOKA database users: user name, first name, last name, and email address;
- Creating an internal web-based interface for FBI users; and
- Providing a web-based interface for state programs and direct contributing law enforcement agencies to submit data via LEEP.

(c) The type of information collected, maintained, used, or disseminated by the system:

As stated above, the LEOKA Program collects information regarding incidents in which law enforcement officers are killed and assaulted in the line of duty. The detailed LEOKA data contains information about the victim officer who was killed or assaulted during the incident which is being reported. This data includes the officer's name, rank, total law enforcement experience, date of birth, gender, race, height, weight, and circumstances surrounding the incident. Offender data is also collected including the offender's name, date of birth, gender, race, height, weight, place of birth, current or known residence, Universal Control Number (UCN),[3] and criminal history record information from the Next Generation Identification (NGI) System.[4] The LEOKA Program receives the incident and biographic information from the victim officer's law enforcement agency or an FBI field office. As stated above, the program uses the information to provide a public view of law enforcement officers killed and assaulted through its annual statistical publication and summaries available at https://ucr.fbi.gov/leoka-resources. In the future, LEOKA may also release its statistical information via the CDE. The statistical publications do not include directly identifying information, such as name and date of birth.

---

[1] The UCR Program and the CDE have separate privacy documentation.
[2] LEEP is covered by separate privacy documentation.
[3] The UCN, also known as the FBI Number, is a unique identification number assigned to each fingerprint submission to the NGI system.
[4] The NGI system has separate privacy documentation.

Additionally, the LEOKA Program uses the incident information listed above to identify specific cases to be used in each of its research studies. For example, program staff may search the LEOKA database to identify all cases within a 10-year period which involved the victim officer being feloniously killed in ambush style attacks. Those incidents are then reviewed, on a case-by-case basis, to determine whether or not the offender is still living and incarcerated. After the sample cases are determined, LEOKA Program staff conduct research to locate the offenders and victim officers. The team then travels to their locations to administer questionnaires and conduct interviews regarding the incident. Before conducting the interviews, each participant signs a consent form. With the participants' consent, the interviews are recorded, transcribed, and used for research and training purposes. Information gathered through LEOKA research, such as videotaped interviews, are maintained by the LEOKA Program separately from the LEOKA database. The LEOKA Program also maintains an OSAT Microsoft Access database to retain information pertinent to OSAT such as training dates, locations, number of anticipated attendees, number of actual attendees, and class evaluations. FBI instructor names are the only PII in the OSAT database. Other information required for the OSAT staff to perform their daily functions, such as policy documents, budget spreadsheets, and location priority maps, is maintained in a variety of Microsoft Excel spreadsheets, Microsoft Word documents, and other computer and hard-copy files. The OSAT database and other information is only available to LEOKA Program staff and OSAT personnel. Class evaluations may be retuned with an attendee's name; however, once the evaluations are used for numeric tabulations, the evaluations are destroyed.

The LEOKA database collects point of contact information for individuals who are submitting data and the head of the agency for which data is submitted, such as name, telephone number, and email address. The LEOKA database 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 database includes a record status history which shows the user who created an entry and the user who last modified an entry.

(d) Who has access to information in the system:

Only FBI personnel have direct access to all information in the LEOKA database. Access is role based and managed by LEEP. To submit information into the LEOKA database, contributing law enforcement agencies must receive a LEOKA reference number and reference key from the LEOKA Program. Each LEOKA incident has a unique reference number and reference key. With the reference number and reference key, contributing law enforcement agencies input the LEOKA incident information; however, once the data is submitted, the law enforcement agencies cannot access the incident information in the database unless the LEOKA Program staff revert an incident to pending status. LEOKA Program users will have access to view and manipulate the data within the LEOKA database. This will allow the LEOKA Program to create statistical reports and develop training materials. All finalized incident reports will also be stored in Sentinel.[5]

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

Statistical LEOKA data and incident summaries, which have been cleared for public release, will continue to be made public through publications on fbi.gov or the CDE. Publicly released information will not include directly identifying information such as victim and offender names and dates of birth. Additionally, local, state, tribal, federal, and international law enforcement agencies may request statistical LEOKA information to perform their own research on specific topics of interest, (e.g., use of body armor, weapon information, etc.) In 2017, the LEOKA Program received 49 requests from these entities. Directly identifying information on living individuals involved in LEOKA incidents will only be accessible by FBI personnel. For condolence purposes, the names of deceased officers and associated agency head names are shared with law enforcement agencies through the LEOKA Program's Community of Interest within JusticeConnect on LEEP.

Extra information obtained by the LEOKA Program pursuant to research activities (e.g. videotaped interviews, protocol questionnaires) is only accessible to LEOKA Program staff and FBI research partners who have been approved by the FBI's Institutional Review Board (IRB)[6] and have signed data transfer agreements. Information derived from the research is used to create training materials for the LEOKA Program's OSAT courses. When provided consent from participating victim officers and offenders, portions of the videotaped interviews may be used in OSAT. Research information may also result in publications 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.

Point of contact information collected with LEOKA incident submissions is used to contact submitting agencies for clarification regarding their incident submissions to verify and assure the accuracy of LEOKA data. Generally, only FBI personnel supporting the LEOKA program have access to the point of contact information for LEOKA incident submissions. As stated above, for condolence purposes, the name of the agency head for an agency with a deceased officer is shared with other law enforcement agencies via LEEP.

Audit logs for the LEOKA database are only available to information technology (IT) staff who monitor the logs for security and access issues. Audit logs specific to the LEOKA database are alert based. Additional audit logs for access to LEEP and the CJIS Unclassified Network (CJIS UNet) are monitored daily. All LEOKA database users can access the record status history for an incident to which they have access.

(e) How information in the system is retrieved by the user:

Every incident in the LEOKA database has a unique LEOKA reference number and reference key. When a law enforcement officer is killed or assaulted, the LEOKA Program staff create an incident in the LEOKA database. The LEOKA reference number and reference key for that incident

---

[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 that the health, safety, well-being and legal rights of humans who are the subjects of research sponsored by the FBI are protected.

are then provided to the law enforcement agency of the involved officer. After accessing the LEOKA database via LEEP, the law enforcement agency retrieves the incident by the LEOKA reference number and reference key and then adds the pertinent information to the entry. Law enforcement agencies can only retrieve one incident at a time, and only via LEOKA reference number and reference key.

LEOKA Program staff and FBI IT personnel can retrieve information from the LEOKA database by LEOKA reference number and reference key, by username of the last user to access an incident, or by username of the individual who created the incident. The LEOKA database can also generate reports based on any data element collected. For example, the LEOKA staff can retrieve a list of all officers killed within a given year by running a report on victim officer name and providing a date range.

LEOKA staff can retrieve information from the OSAT database based on any data field in the database (e.g. training location, trainer name, number of attendees).

Audit logs can be retrieved by username or federated user ID.

(f) How information is transmitted to and from the system:

Currently, the victim officer's agency or an FBI field office completes the applicable LEOKA Program Forms 1-701 and/or 1-701a[7] with the detailed LEOKA incident data and electronically transmits, emails, mails, or faxes the form to the LEOKA Program. The LEOKA staff then manually enter the LEOKA data into the LEOKA database. With the new LEOKA database, victim officers' law enforcement agencies will be able to automatically submit the LEOKA incident data into the database. Participating law enforcement agencies will log into the LEEP and access the LEOKA web based application. Using the LEOKA reference number and reference key provided by LEOKA Program staff, participating agencies can then access their incident and manually enter the information into the LEOKA database using web forms. Law enforcement agencies can also complete a fillable portable document file (.pdf) form and provide the completed .pdf form to the LEOKA Program. Upon receipt, the LEOKA Program can ingest the .pdf form into the LEOKA database.

Internal LEOKA CJIS UNet[8] users will access the LEOKA web application directly from CJIS UNet. LEOKA staff can also export incidents and other LEOKA database generated reports in .pdf format.

(g) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects):

The LEOKA database will be a standalone database within the CJIS Common Operating Environment. The web based user interface is accessible to external users via LEEP. Internal LEOKA

---

[7] LEOKA's data collection is subject to the Paperwork Reduction Act and therefore undergoes OMB review and approval. OMB recently renewed the data collection (OMB No. 1110-0009).
[8] CJIS UNet is covered by separate privacy documentation.

staff can access the user interface via CJIS UNet. Aggregated statistical information from the LEOKA database will also be provided to the CDE either manually by the LEOKA Program staff or through a technical push from the LEOKA database.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security		Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID	x	Credit card			
Other identifying numbers (specify): Universal Control Number (UCN), LEOKA reference key and reference number					

General personal data					
Name	x	Date of birth	x	Religion	
Maiden name		Place of birth	x	Financial info	
Alias	x	Home address		Medical information	
Gender	x	Telephone number	x	Military service	
Age	x	Email address	x	Physical characteristics	
Race/ethnicity	x	Education	x	Mother's maiden name	
Other general personal data (specify): criminal history record information					

Work-related data					
Occupation		Telephone number	x	Salary	
Job title	x	Email address	x	Work history	
Work address	x	Business associates			
Other work-related data (specify): officer's rank					

Distinguishing features/Biometrics					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify): height, weight					

System admin/audit data

System admin/audit data							
User ID	x	Date/time of access	x	ID files accessed	x		
IP address	x	Queries run	x	Contents of files	x		
Other system/audit data (specify): N/A							

Other information (specify)
LEOKA incident submissions also include details surrounding the line-of-duty assault or killing, such as location, date/time, circumstances, weather conditions, location of injuries, type of weapons, body armor usage, number of rounds fired, offender details, etc.

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax	x	Online	x
Telephone	x	Email	x		
Other (specify): 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.					

Government sources					
Within the Component	x	Other DOJ components	x	Other federal entities	x
State, local, tribal	x	Foreign			
Other (specify): N/A					

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

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate

threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

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, the data collected by the LEOKA Program comes directly from the law enforcement agencies of the victim officers and is not taken from an outside source. In addition, the data submitted is checked for inconsistencies by comparing the data provided by the submitter and the incident details included in the attached narrative or incident report regarding the incident. If inconsistencies in the data or incomplete items are identified, further clarification is requested from the submitting agency point of contact. If a victim officer is killed, a representative of his or her agency submits the data via one of the two LEOKA collection forms. If a victim officer is assaulted, it is possible he or she will complete the collection form and submit it to the LEOKA Program. 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 information used for research studies is accurate.

To further mitigate privacy risks, the FBI collects only the minimal amount of information needed to provide a comprehensive view of LEOKA incidents. Information collected by the LEOKA Program 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 Advisory Policy Board (APB)[9] and guidance from the Office of Management and Budget to ensure the program only collects the minimum amount of information needed. Although the FBI collects directly identifying information about officers and offenders (e.g. name, date of birth), this information is not publicly released on living individuals; data collected by the LEOKA Program is published and released in an aggregated format.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities	x	For administrative matters

[9] 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 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.

	To conduct analysis concerning subjects of investigative or other interest	x	To promote information sharing initiatives
x	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
x	Other (specify): To gather information to develop OSAT.		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

The LEOKA Program's mission is to reduce incidents of law enforcement officer deaths and assaults by providing data, research, and instructional services relative to law enforcement safety. The LEOKA data collection not only provides valued information to be used by the program, it also benefits the law enforcement agencies in several ways. Representatives within those agencies use the data to design new policies or modify existing ones, determine resources needed by the officers or if additional personnel is required, and to develop officer safety training specific to their agency.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

	Authority	Citation/Reference
X	Statute	28 U.S.C. § 534
	Executive Order	
X	Federal Regulation	28 CFR 0.28(f)
	Memorandum of Understanding/agreement	
X	Other (summarize and provide copy of relevant portion)	*CJIS Security Policy* (available at http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view); CJIS User Agreement; and LEEP Rules of Behavior

3.4 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. Incidents flagged as deleted from the LEOKA database will be maintained within the database audit

logs. Audit logs are maintained on the database for seven days and then moved to a physically separate system where they are kept for one year. Publications from the LEOKA submissions will be retained permanently. Information regarding the LEOKA database (e.g. system documentation, snapshots of the database, etc.) will be transferred to the national archives and stored as "permanent" information.

LEOKA research materials such as videos, transcripts, and aggregated data is kept for a period of three years after the conclusion of the study. Some videos of interviews conducted during the research are edited and become part of the OSAT curriculum. Those videos and training materials are retained for twenty-five years.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.) [In addition to providing a narrative answer, please consult the ISSO/ISSM for the system's NIST 800-122 PII Confidentiality Risk Level, and check the applicable Confidentiality Safeguard Security Controls.]

The greatest privacy risk to LEOKA information is the potential for unauthorized access to or misuse of directly identifying information about officers and offenders. To mitigate this risk, direct access to the LEOKA database is limited to FBI personnel. Law enforcement agencies may submit data via the LEEP portal, but they can only access their specific incident after receiving a reference key and a reference number. After submission, the law enforcement agency will receive an email containing a copy of the form they submitted but will no longer have access to that specific submission or any previous submissions. Risks of unauthorized access or misuse of LEOKA information are further mitigated through the use of two-factor authentication to log into LEEP and role based access controls which limit access to the full database to only FBI personnel. All LEOKA database users must agree to the LEEP Rules of Behavior which include provisions for termination of access if the system is misused. Administrative access to the LEOKA database is controlled through user identification and two-factor authentication to the workstation. All LEEP users and individuals with access to the LEOKA database have completed information security and privacy training. The training addresses the roles and responsibilities of the users of FBI systems and raises awareness of the sensitivity of the information contained therein and how it must be handled to protect privacy and civil liberties. All LEEP users are vetted annually to ensure that they meet LEEP membership criteria.[10] Persistent monitoring of LEEP audit and security logs ensures that any unauthorized attempts to access LEEP are quickly identified and resolved.

To further reduce risks to privacy associated with the collection of officers' and offenders' information, the LEOKA program limits the information it makes publicly available. Although the LEOKA program 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.

---

[10] LEEP's Privacy Impact Assessment provides more detail on the vetting process.

Similarly, more detailed information collected during research, such as officer and offender interviews, are not publicly released. More detailed information collected during research is used to develop OSAT materials, which the LEOKA program provides only to law enforcement representatives. OSAT materials are also available to law enforcement personnel and other authorized LEEP users via LEEP. The LEOKA program obtains consent from officers and offenders before using any video clips during OSAT.

PII Confidentiality Risk Level:

☐ **Low** ☑ **Moderate** ☐ **High**

- Is the system protected as classified; or
- Does the system involve intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system; or
- Is the system critical to the direct fulfillment of military or intelligence missions (excluding routine business or administrative applications, e.g., finance, logistics, personnel management)?

☐ **Yes** ☑ **No**

If Yes, the system meets the NIST 800-59 definition of a National Security System.

Access controls

x	Access Enforcement: the system employs role-based access controls and enforcement mechanisms for PII.
x	Separation of Duties: users of de-identified PII data are not also in roles that permit them to access the information needed to re-identify the records.
x	Least Privilege: user roles enforce the most restrictive set of rights/roles for each user group.
x	Remote Access: remote access is prohibited or limited to encrypted communication channels.
x	User-Based Collaboration and Information Sharing: automated mechanisms are in place for matching PII access authorizations to access restrictions, such as contractual/MOU/MOA requirements. External LEOKA database users can only access the incidents for which they have received the reference key and reference number.
x	Access Control for Mobile Devices: access to PII is prohibited on mobile devices or limited so that data can only be accessed on mobile devices that are properly secured and regularly scanned for malware.

Audit controls

x	Auditable Events: access to PII is audited for unauthorized access.
x	Audit Review, Analysis, and Reporting: audit records are regularly reviewed for inappropriate or unusual activity affecting PII; such activity is investigated and reported; and responsive action and appropriate mitigation is taken.
[Audit logs will track system and Database administrator access of information. Tripwire will monitor system file access for changes. The information system logs user access and tracks changes made to LEOKA incident submissions. Database specific logs are alert driven. CJIS UNet and LEEP audit logs are monitored daily.]	

Identification and Authentication controls

x	Identification and Authentication: users are uniquely identified and authenticated before accessing PII; remote access requires 2-factor authentication and 30-minute "time-out" functionality.

Media controls

x	Media Access: access to system media containing PII (CDs, USB flash drives, backup tapes) is restricted.
x	Media Marking: media containing PII is labeled with distribution/handling caveats.
x	Media Storage: media containing PII is securely stored.
x	Media Transport: media is encrypted or stored in a locked container during transport.
x	Media Sanitation: media is sanitized prior to re-use.

Data Confidentiality controls (Be sure to also discuss in Section 1(f).)

x	Transmission Confidentiality: information is encrypted prior to transmission or encrypted transmission is used. (**Required if the system meets the NIST 800-59 definition of a National Security System**.)
x	Protection of Information at Rest: Information in the LEOKA database is stored within physically secure locations.

Information System Monitoring

x	Information System Monitoring: network boundaries are automatically monitored for unusual or suspicious transfers or events

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	x	x	x	
DOJ components	x	x		
Federal entities	x	x		
State, local, tribal gov't entities	x	x		
Public	x	x		Publication of aggregated statistical data and case summaries. No directly identifying information is disclosed to the public.

Private sector	x	x		
Foreign governments				
Foreign entities				
Other (specify):	x			Upon request, LEOKA 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.

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.) [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

The LEOKA Program collects details regarding law enforcement officer line-of-duty deaths and assaults occurring nationwide and shares that national picture with the law enforcement community, in the hopes of preventing future line-of-duty deaths and assaults. To meet this goal, LEOKA collects PII on officers and offenders; however, the LEOKA program mitigates privacy risks by controlling access to the PII it collects. Direct access to the LEOKA database is limited to FBI personnel. Law enforcement agencies may submit data via the LEEP portal, but can only access their specific incident after receiving a reference key and a reference number. After submission, the law enforcement agency receives an email containing a copy of the form it submitted but no longer has access to that specific submission or any previous submissions.

The LEOKA Program uses the information it collects 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 approved research partners. All research projects and partners are reviewed and approved by the FBI's IRB. 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 the storage of the information, limiting the use of the data provided, and setting forth the destruction requirements once the research project is complete. Any video clips of interviews or PII disclosed during training is only disclosed by consent from the involved officers or offenders. Names of deceased officers and agency heads are provided to the law enforcement community solely for condolence purposes.

The LEOKA Program does release information publicly; however publicly released information is limited to an aggregated view of the data collected and case summaries without directly identifying information, such as name and date of birth. The LEOKA Program electronically releases publicly available information via fbi.gov and the CDE. Upon request from specific individuals, only redacted incident information is provided. This could include a copy of the database minus directly identifying information. The PII redacted before release includes: names, birth dates, addresses, agency incident or case numbers, offender's FBI number, offender's place of birth, offender's date of arrest, and offender's location of death.

To prevent unauthorized access to the LEOKA database, all FBI workstations and servers that access the LEOKA database are secured in accordance with FBI Security Division requirements and are verified before establishing network connectivity. In addition, all hardware is housed within FBI facilities that have achieved site security accreditation. Only authorized FBI personnel and/or contractors may have access to the FBI workstations and servers. Contributing law enforcement agencies can access the LEOKA database via LEEP, which requires two factor authentication. The information/data is further protected by role-based controls and Access Control List(s) at the group and individual level. Logging and auditing procedures are performed as required. The risk of unauthorized access is further mitigated because the maintenance and dissemination of information must comply with provisions of any applicable law, regulation, or policy.

All users are notified through warning banners and by agreeing to the LEEP Rules of Behavior that they are subject to periodic, random auditing of their activities on LEEP and all FBI information systems. This awareness discourages unauthorized or non-work related attempts to access data. Audit logs capturing user access to LEEP are reviewed daily. Unauthorized attempts to access LEEP trigger alerts which are reviewed in real-time. All other system logs are reviewed weekly. For Privileged Users, the LEOKA database is a password-protected system, which in itself helps guard against unauthorized access and disclosure. Before being granted an account, privileged LEOKA database users are required to attend mandatory training. The training includes FBI standard operating procedures, which further guard against improper access or disclosure of information. Privileged users are trained in the appropriate use and access of the data.

The risk of misuse of LEOKA information is further mitigated through auditing and training. System audits are facilitated by user logs, monitoring system use, and user activity. The use of unique User IDs and strong passwords makes it difficult for a user to gain unapproved access or a heightened level of access. User access to information within the LEOKA database 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 (i.e. reference key and reference number) can access incident information in the LEOKA database. If an individual does not have an incident's reference key and reference number, the individual will not be able to view that data. In addition, once an incident is submitted, only FBI personnel can view the incident information. The LEOKA database contains audit functions that can be used to detect improper use and/or access. All user and administrator actions are logged. Anomalous behavior or misuse of the database 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 database 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 users with access to the LEOKA database 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. LEOKA database users acknowledge that they understand sanctions may be applied for intentional misuse of the LEOKA database.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
X	Yes, notice is provided by other means.	Specify how: Point of Contact Information: The LEOKA database includes a Privacy Act statement on the home page informing incident submitters of the purpose for collecting their information and how it will be used. A Privacy Act Statement is also linked at the bottom of the LEEP homepage.
X	No, notice is not provided.	Specify why not: Discretion for incident submittal lies with the involved officer's law enforcement unit/department. Similar to the UCR system, law enforcement units/departments do not notify individuals involved in the incidents (law enforcement or civilian) that the information is being submitted.

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

x	Yes, individuals have the opportunity to decline to provide information.	Specify how: The FBI UCR Program is a voluntary program. Law enforcement agencies are not required to submit data. Since the LEOKA Program is part of the UCR Program, participation is also voluntary and no agency can be required to provide information in regard to law enforcement officer deaths and assaults. Upon login to LEEP, users choosing to submit an incident specifically agree to a government system notice informing them that they have no reasonable expectation of privacy regarding their activities on a government system and that their use of the government system may be monitored, intercepted, searched, and/or seized.

X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: Similar to the UCR system, law enforcement units/departments do not provide individuals involved in the incidents (law enforcement or civilian) with the ability to decline submission.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

X	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how: Point of Contact Information: The LEOKA database requests that incident submitters provide their names, telephone numbers, and email addresses as well as the names, telephone numbers, and email addresses of their agency heads; however, this information is not required to submit a LEOKA incident. All officers and offenders who participate in LEOKA research projects consent to be interviewed and to the use of their information for OSAT purposes.
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Similar to the UCR system, law enforcement units/departments 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. All users accessing the LEOKA database agree to a government system notice informing them that they have no reasonable expectation of privacy regarding their activities on a government system and that their use of the government system may be monitored, intercepted, searched, and/or seized.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why

not.

The purpose of the LEOKA Program is to collect information regarding law enforcement line-of-duty assaults and deaths and to use this information to provide an aggregated view of such incidents and to develop OSAT. The submission of incidents to the LEOKA program is voluntary, and discretion for submittal lies with the involved officer's law enforcement agency. Similar to the UCR system, the LEOKA program does not notify individuals involved in the incident (law enforcement or civilian) that the information is being submitted nor does it request their consent. Although the LEOKA program collects directly identifying information about officers and offenders, this information is not publicly available. Rather, the LEOKA program uses collected information to provide an aggregated view of LEOKA data. This Privacy Impact Assessment provides notice to the public and law enforcement agencies that the FBI collects information about law enforcement line-of-duty assaults and deaths.

The LEOKA database includes a Privacy Act statement informing users why the information (including their contact information) is being collected and how their contact information will be used. All users accessing the LEOKA database also 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. 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.

Section 6: Information Security

6.1 Indicate all that apply.

X	A security risk assessment has been conducted.
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: Security Requirements Traceability Matrix (SRTM), National Institute of Standards and Technology (NIST) 800-53
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: Active system administration and log reviews, automated monitoring, IBM Tivoli Identity Manager (ITIM), Enterprise Security Operations Center (ESOC)
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: The LEOKA database is accredited as part of the CJIS UNet. CJIS UNet most recently received an ATO in October of 2016.
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: RSA, Tripwire, and Nagios monitoring, detection, investigative products
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.
X	The following training is required for authorized users to access or receive information in the system:

	x	General information security training
	x	Training specific to the system for authorized users within the Department.
		Training specific to the system for authorized users outside of the component.
		Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure. [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

The LEOKA database is accredited as part of the CJIS UNet. As part of the Security Assessment and Authorization (SAA) process, the CJIS UNet included a NIST 800-53 security control baseline at the HIGH/MEDIUM/HIGH impact level of assurance (LOA). Access to the system is restricted as required by established security controls. Security controls are continually assessed during the application/system development life cycle for compliance and to ensure appropriate mitigations strategies have been implemented commensurate with the HIGH/MEDIUM/HIGH impact LOA to protect the confidentiality, integrity, and availability of data.

The CJIS Information Assurance Unit assigned and provided an Information Systems Security Officer (ISSO) and an Information Systems Security Engineer (ISSE) to oversee the SAA process for the CJIS UNet. The ISSO and ISSE are responsible for ensuring the day to day implementation, continuous monitoring, and maintenance of the security configuration, practices, and procedures for the CJIS UNet and the LEOKA database. The ISSO/ISSE assists the operational staff and Program Office to make certain that system security documentation is developed, maintained, reviewed and updated to reflect changes to the risk posture and privacy impact of the CJIS UNet. The ISSO/ISSE team also identify and coordinate appropriate correction or mitigation actions to track the timely completion of changes to the system and applications. Please see section 4.2 for additional access and security control descriptions.

ISSOs and System Security Administrators continually review the security controls per the FBI Security Assessment and Authorization Policy Guide and also use the National Institute of Standards and Technology special publication 800-53A, revision 4 for expanded definitions and guidance. The ISSO is required to review security controls annually. Security Control Risk Assessment 5 focuses 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 CJIS UNet system is high 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.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: **JUSTICE/FBI-004,** *FBI Online Collaboration Systems,* 82 FR 57291 (Dec. 4, 2017), and **JUSTICE/FBI-002,** *The FBI Central Records System,* 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).
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

As discussed above, contributing law enforcement agencies can retrieve incidents from the LEOKA database with the unique LEOKA reference number and reference key. Contributing law enforcement agencies can only retrieve one incident at a time, and only via the LEOKA reference number and reference key.

LEOKA Program staff and FBI IT personnel can retrieve information from the LEOKA database by LEOKA reference number and reference key, by username of the last user to access an incident, or by username of the individual who created the incident. The LEOKA database can also generate reports based on any data element collected. For example, the LEOKA staff can retrieve a list of all officers killed within a given year by running a report on victim officer name and providing a date range.

LEOKA staff can retrieve information from the OSAT database based on any data field in the database (e.g. training location, trainer name, number of attendees).

Audit logs can be retrieved by username or federated user ID.