Federal Bureau of Investigation

Privacy Impact Assessment
for the
[National Use-of-Force Data Collection (NUOFDC)]

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

Approved by: Brian Young
Unit Chief
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: [June 20, 2024]

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 National Use-of-Force Data Collection (NUOFDC), a collection within the Uniform Crime Reporting (UCR) Program, consists of reports of any use of force by a law enforcement officer that results in the death or serious bodily injury of a person, as well as when a law enforcement officer discharges a firearm at or in the direction of a person. State, local, tribal, and territorial law enforcement agencies voluntarily provide the FBI with information regarding the use of force by their law enforcement officers. Section 6 of Executive Order 14074, Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety, requires federal law enforcement agencies to submit data to the NUOFDC. The FBI compiles and publishes statistical data on the use of force. This promotes transparency between law enforcement and the communities they serve. Additional information about the National Use-of-Force Data Collection is available online at fbi.gov.

While the NUOFDC is not designed to collect directly identifiable information about individuals other than system users, the combination of the data elements might allow, in certain circumstances, individuals involved in the incidents to be identified. This privacy impact assessment addresses the privacy risks associated with the information collection, including the ability to link the data and the decisions made to limit, to the extent possible, the ability to indirectly identify the officers and subjects involved in the use of force incidents.

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 FBI compiles and publishes statistical data on the use of force. This promotes transparency between law enforcement and the communities they serve. The NUOFDC collects and reports any use of force by a law enforcement officer that results in the death or serious bodily injury of a person, as well as when a law enforcement officer discharges a firearm at or in the direction of a person.

The NUOFDC's goal is to produce a national picture of the trends and characteristics of use of force by law enforcement officers (as defined by the Law Enforcement Officers Killed and Assaulted program) and not to offer insight into single use of force incidents. The collection and reporting include incidents involving use of force resulting in the death or serious bodily injury of a person, as well as when a law enforcement officer discharges a firearm at or in the direction of a person. The data collected by the UCR Program includes information on the officers, the subjects, and the circumstances surrounding the incident itself. The data collection focuses on information readily

known and attainable by law enforcement with the initial investigation following an incident rather than any assessment of whether the officer acted lawfully or within the bounds of department policies. Publications and releases from the data collection provide for the enumeration of fatalities, nonfatal encounters that result in serious bodily injury, and firearm discharges by law enforcement. The collected data elements provide context around use of force incidents and assist agencies in identifying patterns among use of force incidents. For example, the collection of height and weight of officers and subjects may reveal whether there is a relationship between a disparity in size and an officer's use of force against a subject. In addition, targeted analyses could potentially identify those law enforcement agencies with "best practices" in comparison with their peers as an option for further study.

The NUOFDC will facilitate important conversations with communities regarding law enforcement actions in relation to decisions to use force. This data collection works in concert with recommendations from the President's Task Force on 21st Century Policing to strengthen community policing and trust among law enforcement officers and the communities they serve. Given a growing desire among law enforcement organizations to increase their own transparency and embrace principles of procedural justice, this collection will provide data on a broader scope of use of force incidents, including the use of force in nonfatal instances.

The NUOFDC collects data submitted by federal, state, local, tribal, and territorial agencies regarding their involvement in use of force incidents. Law enforcement agencies have two methods through which to submit data. The first method involves the submitter authenticating into the Law Enforcement Enterprise Portal (LEEP)[1] and, after receiving proper authorization, opening the NUOFDC application and submitting the data. The second method allows agencies to use a machine-to-machine interface to send the FBI a file via the Enterprise File Transfer Service's (EFTS) Secure File Transfer Protocol (SFTP), which the NUOFDC system ingests. The first method restricts submittals to one incident at a time, while the second method allows for multiple incidents to be sent and ingested simultaneously.

The FBI uses incident information from the NUOFDC system to create reports to aid in the national dialogue regarding frequency, locations, and reasons for law enforcement involved use of force incidents. The FBI publishes statistical data from the collection.

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

	Authority	Citation/Reference
X	Statute	28 U.S.C. § 534
X	Executive Order	14074
X	Federal Regulation	28 CFR 0.85(f)

[1] 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, including the National Use-of-Force Data Collection system, and ensuring that only authenticated users have access to those systems and services. To participate in LEEP and gain access to the National Use-of-Force Data Collection system, users must provide six identifying pieces of information: User ID, First Name, Last Name, User's Agency Email Address, User's Agency Telephone Number, and Employer/Agency Name. LEEP has separate privacy documentation.

	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	President's Task Force on 21st Century Policing

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

The NUOFDC collects information about officers and subjects involved in use of force incidents. Each law enforcement agency reports information for its own officers connected to use of force incidents that meet the criteria of the data collection. The FBI uses a closed-end response survey to collect data elements, which are most easily explained as three types of information: incident information, officer information, and subject information.

Incident information: Information collected about the incident includes the date and time of the incident, the number of officers who applied actual force during the incident, the location of the incident (either street address or latitude and longitude coordinates), the type of location (e.g., business, residence, parking lot), whether the officer approached the subject, whether the incident was an ambush of law enforcement, the reason for initial contact between the subject and officer, whether an officer acting in a supervisory capacity was present or consulted during the incident, and if charges were filed against the subject by a prosecutor. Information about whether charges were filed against the officer or agent is not collected.

Officer information: Information collected regarding the officers who applied force during the use of force incident includes the officer's age, sex, race, ethnicity, height and weight; the officer's years of service as a law enforcement officer; whether the officer was a full-time law enforcement officer; whether the officer was on duty at the time of the incident; whether the officer discharged a firearm; whether the officer was injured or died from injuries sustained in the incident; and, if applicable, the type of injury the officer received. The FBI does not collect the officer's name, date of birth, social security number and other similar forms of personally identifiable information (PII) that could directly identify the officer. However, descriptive information collected about the officer, when combined with the incident information and other publicly available information, such as media reports, may allow the officer information to be linked back to a specific law enforcement officer.

Subject information: Information collected regarding the subject involved in the use of force incident includes the subject's age, sex, race, ethnicity, height, and weight range; whether the use of force resulted in injury to the subject or the subject's death; the type of injury the subject received; the type of force used upon the subject; whether the subject resisted police interaction; whether the subject was

threatening the officer or another individual; how the subject resisted and the type of weapon the subject had, if applicable; whether the subject was suffering from an apparent or known impairment or physical condition (e.g., mental health condition, drug impairment, alcohol impairment); and whether the subject was armed or believed to be armed. The FBI does not collect the officer's name, date of birth, social security number and other similar forms of PII that could directly identify the officer; however, the information collected, when combined with the incident information and other publicly available information, such as media reports, may allow the subject information to be linked back to a specific individual.

The NUOFDC system also collects and maintains information pertaining to system users including: user's first and last names, phone number, email address, user ID, the user's role within the system, the originating agency identifier (ORI) of the agency for which the user inputs information into the system, the status of the user's account (e.g., enabled, enabled never logged in, disabled, or deleted), and the date the user enrolled into the NUOFDC system. System users include: local law enforcement personnel, state UCR program personnel, and FBI personnel supporting the NUOFDC. System privileges are based on a combination of role and account privileges. User account information is used for account provisioning purposes, creating system audit logs, and providing the user's point of contact (POC) information. Access to a specific user's information is role based and is restricted to the user, other users in the user's chain of review, and FBI personnel supporting the NUOFDC including system and database administrators. User information is maintained to provide users and reviewers with POC information, to facilitate generating system reports on items such as which users and agencies have submitted data and which users and agencies have incidents that need to be reviewed, and to allow users to subscribe to system reports and alerts. Users may subscribe to system alerts informing them of actions that need to be taken within the system or to alerts informing them of system performance updates. These system reports and alerts are sent via email from the NUOFDC system.

NUOFDC audit logs collect the user ID of individuals accessing the NUOFDC system, time-stamped events such as attempted logins/logouts, and changes users make to incident submissions. NUOFDC audit logs are accessible only to a limited group of system administrators and are only accessed for auditing purposes or to detect system misuse. NUOFDC audit logs collect information on all changes to data within the system including incident and user account information. Access to this information is role based and is restricted to UCR program office staff and FBI personnel supporting the NUOFDC including system and database administrators. Incident submissions also include a transaction history showing any changes to the submitted incident. Any user with access to the incident can see the incident's transaction history.

(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	Names are collected for system users.
Date of birth or age	X	A, B, C, and D	The NUOFDC collects the age of the officer and the subject.
Place of birth			
Gender	X	A, B, C, and D	For officers and subjects involved in use-of-force incidents.
Race, ethnicity or citizenship	X	A, B, C, and D	For officers and subjects involved in use-of-force incidents.
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			
Work e-mail address	X	A, B, C, and D	For system users only; 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	For system users only; 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	Incident submissions include information about the types of injuries sustained by the subject or officer and whether the subject appeared under the influence of alcohol or drugs.
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information	X	A, B, C, and D	Incident submissions include the officer's years of experience; whether the officer is full-time or part-time; whether the officer was on-duty at the time of the incident, and the ORI assigned to the user's agency.
Employment performance ratings or other performance information, e.g., performance improvement plan			
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	Incident submissions do not include criminal history but do include the suspected criminal activity in which the subject was engaged at the time of the incident and a yes/no on whether criminal charges were filed against the subject (not the officer).

(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
Juvenile criminal records information	X	C and D	Incident submissions do not include criminal history but do include the suspected criminal activity in which the subject was engaged at the time of the incident and a yes/no on whether criminal charges were filed against the subject.
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C, and D	Incident submissions include the location (address or latitude/longitude) at which the incident occurred.
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **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	Audit logs track system and database administrator access of information. The NUOFDC system logs user access and tracks changes made to incident reports including the specific changes within an incident submission (e.g., change of officer's information from on duty to off duty). System users include federal and non-federal government employees; 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	In addition to User ID, audit logs also collect the ORI for the user's agency.
- **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	

(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
- **Contents of files**	X	A, B, C, and D	If an incident is flagged as deleted, the NUOFDC audit log will reflect all information that was in the deleted incident. Tripwire software is used to monitor access and changes to underlying system programming files. Tripwire monitors system file integrity and detects changes in real-time, including identifying who made the changes and when. Tripwire also alerts system administrators to changes of the underlying system configuration files.
Other (please list the type of info and describe as completely as possible):	X	A, B, C, and D	Incident submissions include physical descriptors (height and weight) of the officers and subjects. The NUOFDC system also collects the ORI of the agency submitting incident information and the ORI of other agencies with officers involved in use of force incidents. Incident submissions also include the case ID for the law enforcement investigation.

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

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	X
Phone		Email			
Other (specify): Clarification of the "Online" box being checked: Individuals applying for access to the NUOFDC request access online. Officers and others involved in use of force incidents do not themselves submit information online.					

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

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

Section 4: Information Sharing

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

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**

Within the Component		X	X	FBI personnel supporting the NUOFDC have access to the information based on user role as described below. FBI field office personnel submitting incidents to the NUOFDC have access to their incident submissions.
DOJ Components		X	X	Submitting agencies have continual access to their data through the NUOFDC system. Submitting agencies can download their incident submissions from the NUOFDC.
Federal entities		X	X	
State, local, tribal, territorial gov't entities		X	X	
Public		X		Statistical information from the NUOFDC system will be published at least annually on the Crime Data Explorer (CDE).[2]
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

Federal, state, local, tribal, and territorial law enforcement personnel use LEEP to obtain access to and to authenticate into the NUOFDC system. The NUOFDC system controls the user roles and data access of the users. Depending on assigned permissions, once logged in to the NUOFDC system, users can enter, view, and manage the data.

Local incident contributors assigned by an agency can create, update, and flag as deleted[3] NUOFDC incidents on behalf of their agency; indicate whether an incident for their agency is complete and submit the incident to the next step in the review process; review their agency's incident data and check for data quality errors; submit a bulk load submission of data on behalf of their agency; choose data for inclusion in reports; export data to spreadsheets; and view the transaction history for incidents from their agency.

State program and domain managers can create, update, and flag as deleted NUOFDC

[2] The CDE is a web-based solution that enables the public to view and interact with national UCR data in an intuitive and user-friendly way. The CDE provides UCR data to the public via an interactive website that allows the general public to query, view, and download statistical crime reporting data submitted voluntarily to the national UCR Program. The PIA for the UCR System addresses the CDE.

[3] Users have the ability to flag incidents as deleted. If an incident is flagged as deleted, it is only visible when specifically requested through limited reports and the data export capability.

incidents on behalf of agencies in their state; indicate whether an incident for an agency in their state is complete and submit the incident to the next step in the review process; review their state's incident data and check for data quality errors; submit a bulk load submission of data on behalf of agencies within their state; choose data for inclusion in reports; export data to spreadsheets; add notifications for the reporting status of each agency in their state; and view the transaction history for incidents from their state.

Account managers for federal, state, local, tribal, and territorial law enforcement users of the NUOFDC system can create, update, and delete roles for their NUOFDC users.

In the NUOFDC system, users can only access entries for their assigned ORIs based on the system's authorizations and data access controls.

FBI personnel supporting the NUOFDC and publication have access to information within the system based on their assigned roles. FBI statisticians supporting the NUOFDC can view all entries within the system; create a NUOFDC incident on behalf of a requesting agency; indicate whether an incident is complete and submit an incident for the next step of the review process; review incidents and check for data quality errors; inform data owners if the data needs to be updated; choose data for inclusion in reports; export data to spreadsheets; and view the transaction history for incidents. FBI statistical assistants supporting the NUOFDC and publication can review all incidents and check for data quality errors; inform data owners if their data needs to be updated; set reminders for the user community to review their data for completeness; and view the incident transaction history for incidents. FBI Technical Information Specialists supporting the NUOFDC and publication can export data to spreadsheets; review data and check for data quality errors when the incident is ready for FBI review; inform data owners if their data needs to be updated; receive and review "zero reports" if an agency had no NUOFDC incidents in a given month; and use data for publications. Writers and Editors in the CJIS Division's Multimedia Production Group can export data to spreadsheets. The Multimedia Production Group uses the exported information to produce publications for FBI.gov.

Database administrators are responsible for maintaining the database and can access ORI data in the NUOFDC database. System administrators are responsible for maintaining and monitoring the NUOFDC hardware and software. System administrators do not have access to the incident submissions; however, they are the only individuals with access to user audit logs for the NUOFDC system.

NUOFDC system users can create reports and export data from the system based upon existing permissions to view data. Submitting agencies have access only to their incident submissions. System users will have the ability to customize the export parameters to create a subset of the data by data elements such as, but not limited to, date of incident, ORI, or type of incident (e.g., fatality, serious bodily injury). For FBI publications, information from the NUOFDC system will most likely be retrieved by date of incident. Incident data cannot be retrieved by name or other personal identifier of an individual involved in the incident. Audit logs and user contact information may be retrieved by username or other personal identifier of a system user.

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

Statistical information from the NUOFDC is published and publicly available on the CDE on at least an annual basis. The published statistical information uses aggregated data from incident submissions to the NUOFDC that limit the ability of the reader or user to link information back to a particular individual. For example, agencies submit the specific address location of a use of force incident; however, the published statistics will not include incident information from a specific address. Rather, the location information is used to provide information about use of force incidents to refined geographical presentations such as states, regional areas, or nationally. Information regarding use of force incidents by a specific law enforcement agency will be limited to basic numeric counts of fatal incidents, nonfatal incident, and incidents involving the discharge of a firearm at or in the direction of a person.

In 2017, after consultation with the Office of Management and Budget, the FBI agreed to the following terms of clearance describing the quality standards which apply to the dissemination of NUOFDC information to ensure any statistical publication of the data is nationally representative. For the purpose of these conditions, "coverage rate" refers to the total law enforcement officer population covered by the NUOFDC. In addition, "coverage rate" is considered on both a state-by-state basis, as well as a national scale. "Key variables" include subject injuries received and type of force used. Item nonresponse refers to the percent of respondents that either do not answer the question associated with a key variable or answer "unknown and unlikely to ever be known."

For the first year of collection,

A. If the coverage rate is 80 percent or greater and the item nonresponse is 30 percent or less, no conditions apply to the dissemination of the results.
B. If the coverage rate is between 60 percent and 80 percent or the item nonresponse is greater than 30 percent, the FBI will not release counts or totals but may release ratios or percentages.
C. If the coverage rate is between 40 percent and 60 percent, the FBI may release only the response percentages for the key variables across the entire population and for subpopulations which represent 20 percent or more of the total population.
D. If the coverage rate is less than 40 percent, the FBI will not disseminate results.

In subsequent years, if any combination of conditions C and D are met for three consecutive years, or if condition D is met for two consecutive years, then the FBI will discontinue the collection and explore alternate approaches for collecting the information, for example, by working cooperatively with the Bureau of Justice Statistics to expand their current efforts to collect information on deaths in custody to include law enforcement.

The FBI's UCR Program tracks officer coverage continuously to ensure compliance with the terms of clearance and to better evaluate the current state of the collection. The method is based on agency participation within the NUOFDC System and reported police employee counts associated

with enrolled agencies. The FBI's UCR Program uses this information to both limit releases based on coverage thresholds and plan future developments based on coverage growth rates.

The FBI receives requests for the underlying incident submissions for published NUOFDC information. To respond to these requests while mitigating, to the extent possible, the ability to link incidents to specific officers and subjects, the FBI develops publication policies for both tabular presentations and data files to manage the risk of identity disclosure based upon the "best practices" identified by other federal statistical programs. Best practices may include using a "10-observation" threshold[4] to limit the risk of discovering the identity of an officer or subject. These best practices are always under review for potential improvements or adjustments, and the FBI's UCR Program will be evaluating new and advanced methods for increasing the utility of the data while also considering the privacy implications for all individuals involved. As the data collection develops, the FBI's UCR Program continues to consult with the FBI's Privacy and Civil Liberties Unit regarding the FBI's release of incident level data from the NUOFDC. Incident level data will only be available after the statistical data from the NUOFDC system is published.

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.

User Information: NUOFDC system users receive a Privacy Act statement on the account request form informing them that their information is being collected for account provisioning purposes and that their contact information may be made available to other NUOFDC system users or as set forth in the routine uses covered by the System of Records Notices listed in Section 7.2 below. For user reference, the Privacy Act statement is also linked at the bottom of the NUOFDC system webpage.

Incident Information: Federal, state, local, tribal and territorial agencies submit incidents to the NUOFDC system. The FBI does not collect incident information from the officers or subjects involved and therefore does not notify individuals involved in the incidents (law enforcement or civilian) that the information is being submitted. Although there is a risk that data elements collected by the NUOFDC may be linked with information from other sources to identify a specific officer or subject involved in a use of force incident, the system is designed to produce a national picture of the trends and characteristics of use of force by law enforcement officers and organizations and not to offer insight into single use of force incidents, subjects, or officers. Despite its design focusing on national trends, this project involves the FBI collecting information about law enforcement involved use of force incidents that potentially could be linked to a specific officer or subject.

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

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, rather than the officers and subjects involved in the use of force incidents, determine whether to submit incident information to the NUOFDC. By participating in the NUOFDC, law enforcement agencies consent to the FBI's use of their incident data for statistical publications. All individuals requesting access to the NUOFDC receive notice of how their information will be used. By requesting and receiving access to the NUOFDC, users consent to the collection and use of their information. When logging in to the NUOFDC, all users must 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.

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.

NUOFDC incident information submitted to the FBI does not directly identify individuals involved in the incidents. Partner law enforcement agencies submit information about their incidents, and FBI data quality examiners address any data issues with the submitting agency.

NUOFDC system users 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. The request should include a general description of the records sought, and must include the requester's full name, current address, and date and place of birth. The request must be signed and dated and either notarized or submitted under penalty of perjury. While no specific form is required, requesters may obtain a form (Form DOJ-361) for use in certification of identity, which can be located at the above link. In the initial request, the requester may also include any other identifying data that the requester may wish to furnish to assist the FBI in making a reasonable search. The request should include a return address for use by the FBI in responding; requesters are also encouraged to include a telephone number to facilitate FBI contacts related to processing the request. A determination of whether a record may be accessed will be made after a request is received. In most cases, because FBI does not collect individuals' names, dates of birth, SSNs, etc., from the submitting law enforcement partner agency, the FBI will not be able to confirm whether a specific incident pertains to a specific individual. Such persons will need to go to the submitting agency and seek correction of the data from that agency.

Section 6: Maintenance of Privacy and Security Controls

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

X	**The information is secured in accordance with Federal Information Security Modernization Act 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 ATO for the NUOFDC system expires on November 20, 2025. In the future, the NUOFDC system will be incorporated into the Crime Data Value Stream (CDVS) security boundary which will provide information technology (IT) security controls to all systems and applications within its boundary. The FBI is working toward an ATO for CDVS. **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** All the security controls relevant to the NUOFDC system using NIST Special Publication (SP) 800-37 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	**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 identified critical and high vulnerabilities have been removed. Other 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 0conducted:** 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, training videos and answers to frequently asked questions are available within the NUOFDC system.

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?

Mitigation of potential unauthorized or inappropriate access to the NUOFDC system relies on system security that ensures only authorized users have access to the system. Users access the NUOFDC system via LEEP which requires multi-factor authentication for log on. Role-based controls and access control list(s) at the group and individual level further protect the information in the NUOFDC system.

All users are notified, through warning banners and by signing the *FBI Rules of Behavior* or the *LEEP Rules of Behavior* that they are subject to periodic, random auditing of the searches they performed, when they performed the searches, and what data was accessed or altered. This awareness discourages unauthorized or non-work-related searching and provides awareness of data that has specific handling requirements or sensitivity. The NUOFDC system also maintains audit logs that record the user ID of individuals accessing the system and time-stamped events such as attempted logins/logouts and system configurations. 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. 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. Anomalous behavior or misuse of the NUOFDC system 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 NUOFDC system 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 NUOFDC system must comply with applicable security and privacy protocols addressed 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*. NUOFDC system 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.

UCR Operations staff, ISSOs, and the SSA continually review the IT security controls per FBI policy and also use the NIST special publication 800-53A, revision 5 for expanded definition and guidance. The ISSO is required to review security controls annually. Risk Assessments focus 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 NUOFDC system supports a system-to-system exchange of data using SFTP through EFTS or web services. SFTP uses Public/Private key pairs to uniquely identify the system and protect the data. Web services use certificates to establish a trusted connection to the system and protect the data in transit.

The NUOFDC system resides in 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.)

The FBI retains incident submissions to the NUOFDC permanently. Incidents flagged as deleted from the NUOFDC system remain in the NUOFDC system audit logs. Audit logs are maintained on the system for seven days and then moved to a physically separate system where they are kept for one year. Publications from the NUOFDC submissions are retained permanently. Information regarding the NUOFDC system (e.g., system documentation, snapshots of the database, etc.) will be transferred to the national archives and stored as “permanent” information.

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:

Although NUOFDC incident submissions cannot be retrieved by personal identifier of the individuals involved in the incident, audit logs and user contact information of the user entering the incident data may be retrieved by name or personal identifier of the user and are covered by *Department of Justice Information Technology, Information System, and Network Activity and Access Records*, **DOJ-002**, 86 Fed. Reg. 37188 (Jul. 14, 2021); *Bureau Mailing Lists*, **JUSTICE/FBI-003**, 70 Fed. Reg. 7513 (Feb. 14, 2005), as amended at 82 FR 24147 (May 25, 2017); and *FBI Online Collaboration Systems*, **JUSTICE/FBI-004**, 82 Fed. Reg. 57291 (Dec. 4, 2017).

Section 8: Privacy Risks and Mitigation

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

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

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

The greatest vulnerability created by the collection of NUOFDC incident data exists in the combination of data elements with local knowledge of the incident to potentially identify subjects and officers. For example, if the incident involves a female officer in a jurisdiction that has only one female officer, one may quickly deduce the name of the officer involved. To limit the ability to link incident submissions to specific individuals, information regarding individual incidents is only accessible to the submitters of that data, individuals in the submitter's chain of review of use of force incidents (e.g., state program or domain manager), and FBI personnel supporting the NUOFDC project. FBI publications use aggregated data from incident submissions to the NUOFDC to limit the ability of the reader or user to link information back to a particular individual. For example, agencies submit the specific address location of a use of force incident; however, the published statistics will not include specific address information. Rather, the location information will be used to provide information about use of force incidents to refined geographical presentations such as states, regional areas, or nationally. Information regarding use of force incidents by a specific law enforcement agency will be limited to basic numeric counts of fatal incidents, nonfatal incidents, and incidents involving the discharge of a firearm at or in the direction of a person.

In determining which data elements to collect, the FBI worked with federal, state, local, tribal, and territorial law enforcement partners to balance the need to collect enough information to promote a

national dialogue on officer use of force with the privacy concerns of making the information linkable to specific individuals. For example, the FBI and the Use of Force Task Force determined not to combine this data collection with the Death in Custody Report Act (DCRA) requirements, in part because the DCRA collection broadens the scope of the data collection in ways that are not necessary to meet the purposes of the NUOFDC.

There is an additional risk that information provided to the NUOFDC may not accurately portray the use of force by law enforcement officers. To ensure that publications from the NUOFDC information are accurate, timely, and complete, the NUOFDC relies on law enforcement agencies and state or domain UCR programs to indicate when the incident submissions are available for review and use. The originating agency provides the incident data. Once the agency representative is satisfied that the incident information is complete and ready for publication use, the agency representative approves the incident for further use. For agencies that submit information through their State or domain UCR programs, those UCR programs also have the opportunity to review incident information for completeness and quality. The NUOFDC system allows state or domain UCR programs to indicate when incident information is ready to release for FBI publication. State or domain UCR programs submitting bulk data to the FBI will only submit the data once the State or domain UCR program confirms that the data is ready to use for FBI publications. The FBI's publications will only use incident information that has been approved for further use by the submitting agency and/or the state or domain UCR program.