Federal Bureau of Investigation

Privacy Impact Assessment
for the
National Use-of-Force Data Collection

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

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

Date approved: September 17, 2018

(May 2015 DOJ PIA Form)

EXECUTIVE SUMMARY

The National Use-of-Force Data Collection (NUOFDC), a new collection within the Uniform Crime Reporting (UCR) Program, is being established to collect and report 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. Local, state, tribal, territorial, and federal law enforcement agencies will voluntarily provide the FBI with information regarding the use of force by their law enforcement officers. The FBI will compile and publish statistical data on the use of force. Publication of the use of force data will promote transparency between law enforcement and the communities they serve. Additional information about the National Use-of-Force Data Collection is available online at https://ucr.fbi.gov/use-of-force.

While the system is not designed to collect personally identifiable information (PII) on living individuals other than system users, the aggregation of the data might allow, in certain circumstances, individuals involved in the incidents to be identified. This privacy impact assessment is being conducted in part to explore the effects of the linkability of 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 1: Description of the Information System

PURPOSE:

The National Use-of-Force Data Collection (NUOFDC) is being established to collect and report 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 FBI will compile and publish statistical data on the use of force. Publication of the use of force data will promote transparency between law enforcement and the communities they serve.

DATA COLLECTION:

The NUOFDC will collect data voluntarily submitted by local, state, tribal, territorial, and federal agencies regarding their involvement in use of force incidents. Currently, there is no data collection that nationally tracks incidents involving law enforcement use of force. This data collection works in concert with recommendations from the President's Task Force on 21st Century Policing to strengthen community policing and strengthen trust among law enforcement officers and the communities they serve by providing data to facilitate open dialogue about when and why law enforcement uses force, including the use of force in nonfatal instances. Law enforcement agencies are requested to provide data on a monthly basis so that the FBI can provide a timely national picture of law enforcement use of force.

The data will be submitted by law enforcement agencies via two methods. 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 will be accomplished via a machine-to-machine interface where the submitting agency will send the FBI a file via Secure File Transfer Protocol (SFTP) and that file will be ingested by the NUOFDC system. The first method restricts the submittals to one incident at a time, while the second method allows for multiple incidents to be sent and ingested at one time.

TYPE OF INFORMATION:

The NUOFDC will include information on officers and subjects involved in use of force incidents. Each law enforcement agency will voluntarily report information for its own officers connected to use of force incidents that meet the criteria of the data collection. The data elements will be collected from a closed-end response survey and are most easily explained as three types of information: incident information, officer information, and subject information.

Incident information: Information collected on the incident will include 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, and whether an officer acting in a supervisory capacity was present or consulted during the incident.

Officer information: Information collected regarding the officers who applied force during the use of force incident will include 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 officer's name, date of birth, social security number and other similar forms of Sensitive PII[2] that could directly identify the officer will not be collected. However, descriptive information collected on 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.

---

[1] The 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. In order to participate in LEEP and to 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.

[2] Sensitive PII is Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience or unfairness to an individual.

Subject information: Information collected regarding the subject involved in the use of force incident will include 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. If the use of force incident results in the subject's death, the NUOFDC will also be able to collect the subject's name; however, at this time, this feature will not be viewable to submitting agencies and agencies will not be supplying the subjects' name. If deceased subjects' names are collected in the future, the subjects' names will not be accessible to anyone outside of the Department of Justice, the submitting agency, and agencies in the submitting agency's chain of review. Sensitive PII on subjects for whom the use of force does not result in their death (e.g., name, date of birth) will not be collected. However, the information collected on both types of subjects—those that die, and those that do not die as a result of the use of force—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.

Additionally, the NUOFDC system will collect and maintain information pertaining to system users including: user's first and last names, phone number, email address, username, 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 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, in the future subscribe to alerts informing them of system performance updates. These system reports and alerts are sent via email from the NUOFDC system.

NUOFDC audit logs will 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.

The incident information collected by the NUOFDC system will be used to create reports to aid in the national dialogue regarding frequency, locations, and reasons for law enforcement involved use of force incidents. Statistical data from the collection will be made public. Law enforcement agencies will be able to access the statistical data from the collection online via LEEP.

ACCESS, RETRIEVAL, and TRANSMISSION:

Local, state, tribal, territorial, and federal law enforcement personnel will use LEEP to obtain access to and to authenticate into the NUOFDC system. Once logged into the NUOFDC system, the NUOFDC system will control the authorization/roles and data access controls of the users. The users, based on assigned permissions, will be able to enter, view, and manage the data.

Local incident contributors assigned by an agency have the ability to 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 have the ability to create, update, and flag as deleted Use-of-Force 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 local, state, tribal, territorial, and federal law enforcement users of the NUOFDC system will have the ability to create, update, and delete application roles for their NUOFDC users.

Until the FBI publishes data from the NUOFDC system, law enforcement personnel will only be able to access their own NUOFDC entries based on the system's authorizations and data access controls. Once data is approved by the inputting organization and statistical information is subsequently published by the FBI, any law enforcement entity with access to the system will be able to view the published statistical information in the system and export any data to which it has access. However, the ability to manage the incident level data will remain with the original inputting organization.

FBI personnel supporting the NUOFDC and publication will have access to information within the system based on their assigned roles. FBI statisticians supporting the NUOFDC will be able to

[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.

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 have the ability to 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 have the ability to 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 will be able to export data to spreadsheets. The Multimedia Production Group will use the exported information to produce publications for FBI.gov.

Database administrators are responsible for maintaining the database and are able to access some 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.

Although NUOFDC incident submissions do not contain names on living individuals involved in the incident and may not be retrieved using personal identifiers of individuals involved in the incident, audit logs and user contact information may be retrieved by name or personal identifier of the user entering incident data into the system.

TYPE OF SYSTEM

The NUOFDC system is a standalone general support system and only uses LEEP for individual user authentication.[4] It does not interact with any other systems.

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	

[4] As stated above, NUOFDC also allows machine-to-machine interfaces where submitting agencies send the FBI files via Secure File Transfer Protocol (SFTP) and those files are ingested by NUOFDC.

Employee ID		Passport		Patient ID	
File/case ID	X	Credit card			
Other identifying numbers (specify): 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.					

General personal data					
Name	X	Date of birth		Religion	
Maiden name		Place of birth		Financial info	
Alias		Home address		Medical information	
Gender	X	Telephone number	X	Military service	
Age	X	Email address	X	Physical characteristics	X
Race/ethnicity	X	Education		Mother's maiden name	
Other general personal data (specify): Names, telephone numbers, and email addresses are collected on system users only. The NUOFDC system includes the capability to collect a deceased subject's name. Currently, law enforcement agencies will not be submitting decedents' names. If decedents' names are collected in the future, they will not be shared outside of the Department of Justice, the submitting agency, and agencies within the submitting agency's chain of review. The NUOFDC system will collect location information on where the use of force incident occurred which may reflect an officer's jurisdiction and/or the address of a subject involved in a use of force incident.					

Work-related data					
Occupation	X	Telephone number		Salary	
Job title		Email address		Work history	
Work address		Business associates			
Other work-related data (specify): The NUOFDC system will collect the officer's years of experience and the ORI assigned to the user's agency. The system will collect location information on where the use of force incident occurred which may reflect an officer's jurisdiction and/or the address of a subject involved in a use of force incident.					

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):					

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	X

System admin/audit data					
IP address		Queries run	X	Contents of files	X
Other system/audit data (specify): Audit logs will also collect ORI. Audit logs will 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). If an incident is flagged as deleted, the NUOFDC audit log will reflect the 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 information (specify)

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		Online	X
Telephone		Email			
Other (specify): The system will support a system to system exchange of data using secure file transfer protocol (SFTP) or web services. SFTP uses Public/Private key pairs that are used to uniquely identify the system and protect the data. Web services will use certificates to establish a trusted connection to the system and protect the data in transit.					

Government sources					
Within the Component	X	Other DOJ components	X	Other federal entities	X
State, local, tribal	X	Foreign			
Other (specify):					

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

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.)

The greatest vulnerability created by the collection of this data exists in the aggregation of the data combined with local knowledge of the incident. For example, if the incident involves a female officer in a jurisdiction that has only one female officer, one would quickly be able to deduce the name of the officer involved. To limit the linkability of the data to specific individuals, information regarding individual incidents will only be 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 will use aggregated data from incident submissions to the NUOFDC that will limit the ability of the reader or user to link information back to a particular individual. For example, agencies will 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 will be used to provide information about use of force incidents to refined geographical presentations for 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 local, state, tribal, and federal law enforcement partners to balance the need to collect enough information to promote a national dialogue with the privacy concerns in 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 (DICRA) requirements, in part because the DICRA collection broadens the scope of the data collection in ways that are not necessary to meet the purposes of the NUOFDC.

The NUOFDC also includes the capability for agencies to report the name of deceased subjects involved in a use of force incident. This capability was included within the NUOFDC to allow the Department of Justice to deconflict information reported to the FBI through the NUOFDC and information reported to other Department of Justice agencies, such as the Bureau of Justice Statistics. At this time, the NUOFDC will not collect the name of deceased subjects. However, if the decedents' names are collected in the future, the names will only be shared within the Department of Justice for record keeping purposes and to deconflict statistical collections that have overlapping data elements.

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		For administrative matters
	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		
	Other (specify):		

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 goal of the FBI's data collection on law enforcement officer use of force is to produce a national picture of the trends and characteristics of use of force by a law enforcement officer (as defined by the Law Enforcement Officer Killed and Assaulted Program) and not to offer insight into single use of force incidents. The collection and reporting will 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 will include information on the officers, the subjects, and the circumstances surrounding the incident itself. The data collection will focus on information that is 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 will provide for the enumeration of fatalities, nonfatal encounters that result in serious bodily injury, and firearm discharges by law enforcement. The collected data elements will 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 strengthen 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.

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 0.85(f)
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

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 the NUOFDC will be retained permanently. Incidents flagged as deleted from the NUOFDC system will be maintained within 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 will be 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.

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.)

As discussed above, the greatest privacy risk from the NUOFDC arises from the linkability of the information collected with outside sources of information to potentially identify the officer(s) or subject(s) involved in a specific use of force incident. To mitigate this risk, access to individual incident information is restricted to the submitting agency of the incident, state or domain program managers, and FBI employees supporting the NUOFDC. Access to all information within the NUOFDC system is controlled by user role as outlined in section 1 above.

Statistical information from the NUOFDC will be published and publicly available on fbi.gov on at least an annual basis. Published statistical information will also be made available to law enforcement agencies via LEEP. The statistical information published will use aggregated data from incident submissions to the NUOFDC that will limit the ability of the reader or user to link information back to a particular individual. For example, agencies will 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 will be used to provide information about use of force incidents to refined geographical presentations for 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.

There is an additional risk that information provided to the NUOFDC may not accurately portray the use of force by law enforcement officials. To ensure that publications from the NUOFDC information are accurate, timely, and complete, the NUOFDC relies on law enforcement agencies and state or domain uniform crime reporting (UCR) programs to indicate when the incident submissions are available for review and use. The originating agency will enter the incident data. Once the agency representative is satisfied that the incident information is complete and ready for publication use, the agency representative will approve the incident for further use. State and domain UCR programs will 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.

The FBI anticipates that it will receive research requests for the underlying microdata from use of force incident submissions. To meet research needs while mitigating, to the extent possible, the linkability of data with specific officers and offenders, the FBI will be working with the Federal Committee on Statistical Methodology's Confidentiality and Data Access Committee to develop 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 requiring a data transfer agreement prior to providing microdata for research or using a "10-observation" threshold[5] to limit the risk of discovering the identity of an officer or subject. As the data collection develops, the FBI's Crime Statistics Management Unit will continue to consult with the FBI's Privacy and Civil Liberties Unit regarding the FBI's release of microdata from the NUOFDC. The microdata will only be available after the statistical data from the NUOFDC system is published.

There is also a risk of unauthorized access or misuse of user information within the NUOFDC system. This risk is mitigated by the use of two-factor authentication to log into LEEP and to gain access to the NUOFDC system. It is further mitigated by role based access controls which limit access to user information to the user, other users in the user's agency, other users in the user's chain of review, and FBI personnel supporting the NUOFDC. All NUOFDC users must agree to the LEEP

[5] 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.

Rules of Behavior. Furthermore, all access to the NUOFDC is captured in audit logs which are reviewed for system anomalies.

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**

Access controls

X	Access Enforcement: the system employs role-based access controls and enforcement mechanisms for PII.
	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: The NUOFDC system utilizes role based access controls to restrict individual access to the NUOFDC system and the information it contains.
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 NUOFDC reports.	

Identification and Authentication controls

X	Identification and Authentication: users are uniquely identified and authenticated before accessing PII; remote access requires 2-factor authentication and 20-minute "time-out" functionality.

Time-out functionality is 20 minutes. The access and security controls selected for NUOFDC system are used to establish user roles. The user roles are then assigned to specific users to manage access. Contributing law enforcement agencies can access the NUOFDC system 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.

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

X	Transmission Confidentiality: information is encrypted prior to transmission or encrypted transmission is used.
X	Protection of Information at Rest: Information in the NUOFDC system 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		
DOJ components	X	X		
Federal entities	X	X		
State, local, tribal gov't entities	X	X		
Public				Publication of general statistics
Private sector				
Foreign governments				
Foreign entities				

Other (specify):				As described above, submitting agencies have continual access to their data through the NUOFDC system. Additionally, law enforcement agencies have access to published statistical information from the NUOFDC via LEEP. Statistical information from the NUOFDC system will be published at least annually on fbi.gov.

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.)

Statistical information from the NUOFDC will be shared with the public via publications posted on fbi.gov. Likewise, statistical information from the NUOFDC will be shared with law enforcement agencies via LEEP. Access to the incident level microdata within the NUOFDC is restricted to contributing law enforcement agencies, state and domain program managers, and FBI personnel supporting the NUOFDC. As discussed above, the FBI will be working with the Federal Committee on Statistical Methodology's Confidentiality and Data Access Committee to develop 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. It is anticipated that the publication policies will include a method through which some microdata can be released for research purposes.

All FBI workstations and servers that access the NUOFDC are secured in accordance with FBI Security Division (SecD) requirements and are verified prior to 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 NUOFDC system 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 privileged users are notified through warning banners and by signing the FBI 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 by them in all FBI information systems.

This awareness discourages unauthorized or non-work related searching and provides awareness of data that has specific handling requirements or sensitivity. For Privileged Users, the NUOFDC is a password-protected system, which in itself helps guard against unauthorized access and disclosure. Before being granted an account, privileged NUOFDC system 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 information in the NUOFDC is 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. After completing the training, users are granted protected accounts. User access to information within the NUOFDC computer system and application is strictly controlled to protect privacy and reduce the risk of unauthorized access and disclosure. System access is configured to ensure only personnel with the correct credentials can access the NUOFDC data. If an individual does not have specific access permissions to a particular piece of data, the individual will not be able to view that data. The NUOFDC system 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 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.

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. [User Information]	
X	Yes, notice is provided by other means.	Specify how: User Information: The account request form for the NUOFDC system includes a Privacy Act statement informing potential users of the purpose for collecting their information and how it will be used. The Privacy Act Statement is also linked at the bottom of the NUOFDC application webpage.
X	No, notice is not provided.	Specify why not: Incident Information: Submission of incidents to the NUOFDC system is voluntary. Discretion for submittal lies with the law enforcement unit/department involved. Similar to the Uniform Crime Reporting 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: Utilization and submission of incidents to the NUOFDC system is voluntary. Users and law enforcement organizations may decline to subscribe or submit information on use of force incidents. Additionally, all users specifically agree to a government system notice informing them that they have no reasonable expectation to privacy regarding their activities on a government system and that their use of the government system may be monitored, intercepted, searched, and/or seized.
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: Similar to the Uniform Crime Reporting 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.

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:

X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Similar to the Uniform Crime Reporting system, law enforcement units/departments do not request the consent of the individuals involved in the incident (law enforcement or civilian) prior to submission and do not notify or request consent for utilization of this data. All users accessing the NUOFDC system 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. Additionally, the account request form for the NUOFDC system includes a Privacy Act statement informing potential users of the purpose for collecting their information and how it will be used. The Privacy Act Statement is also linked at the bottom of the NUOFDC application webpage.

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 NUOFDC is to collect statistical information regarding law enforcement use of force incidents. The submission of incidents to the NUOFDC system is voluntary and discretion for submittal lies with the law enforcement agency involved in the use of force system. Similar to the Uniform Crime Reporting system, the NUOFDC does not notify individuals involved in the incident (law enforcement or civilian) that the information is being submitted nor does it request their consent. Information on a use of force incident is submitted voluntarily by the law enforcement agency whose officer was involved in the incident. Although there is a risk that data elements collected by the NUOFDC may be linked with information from other sources to identify a specific officer or subject involved in a use of force incident, as discussed above, 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. This Privacy Impact Assessment provides notice to the public and law enforcement agencies that, 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.

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 7.1 below. For user reference, the Privacy Act statement is also linked at the bottom of the NUOFDC application webpage.

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: Authority to Test (ATT) was awarded on December 21, 2016; Authority to Operate (ATO) was granted on February 16, 2017.

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.
	X		Other (specify): For user reference, training videos and answers to frequently asked questions are available within the NUOFDC system.

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

The NUOFDC system is accredited by the FBI Security Division (SecD). As part of the Security Assessment and Authorization (SAA) process, the NUOFDC system included a NIST 800-53 security control baseline at the LOW/MEDIUM/LOW 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 (SDLC) for compliance and to ensure appropriate mitigations strategies have been implemented commensurate with the LOW/MEDIUM/LOW impact LOA to protect the confidentiality, integrity and availability of data.

The CJIS Information Assurance Unit (CIAU) assigned and provided an Information Systems Security Officer (ISSO) and an Information Systems Security Engineer (ISSE) to oversee the SAA process for the NUOFDC system. 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 NUOFDC Information System (IS). The ISSO/ISSE assists the operational staff and Program Office (PO) 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 NUOFDC system. 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.

Included in the security assessments conducted against the NUOFDC system, members of CIAU assessed the risk of unauthorized access and disclosure to provide a depiction of the risk posture for the system. The NUOFDC system itself inherits many of the management, operational, and technical controls related to the CJIS Enterprise infrastructure and operating environment. The access and security controls selected for NUOFDC system are used to establish user roles. The user roles are then assigned to specific users to manage access. The file system and applications use roles to limit access to sensitive information only to authorized users who have the appropriate role. Specifically, only System Administrators (SA) and System Security Administrators (SSA) have access to PII within audit logs, if it exists. Access to user information within the system is limited to the user, other users in the

user's chain of review, and FBI personnel supporting the NUOFDC.

All FBI workstations and servers that access the NUOFDC information are secured in accordance with FBI SecD requirements and are verified prior to 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 NUOFDC system 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 and reviewed daily. 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 privileged users are notified through warning banners and by signing the FBI 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 by them in all FBI information systems. This awareness discourages unauthorized or non-work related searching and provides awareness of data that has specific handling requirements or sensitivity. For Privileged Users, the NUOFDC is a password-protected system, which in itself guards against unauthorized access and disclosure. Before being granted an account, privileged NUOFDC system users are required to attend mandatory training. The training includes FBI standard operating procedures, which further guard against improper access or disclosure of information. Users are trained in the appropriate use and access of the data.

The risk of misuse of information in the NUOFDC is mitigated by auditing. 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 NUFODC computer system and application is strictly controlled to protect privacy and reduce the risk of unauthorized access and disclosure. System access is configured to ensure only personnel with the correct credentials can access the NUOFDC data. If an individual does not have specific access permissions to a particular piece of data, the individual will not be able to view that data. The NUOFDC system 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 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.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created or has been created in accordance with 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: 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 *DOJ Computer Systems Activity and Access Records*, **DOJ-002**, 64 Fed. Reg. 73585 (Dec. 30, 1999), as amended at 66 Fed. Reg. 8425 (Jan. 31, 2001) and 82 Fed. Reg. 24147 (May 25, 2017); and *Bureau Mailing Lists*, **JUSTICE/FBI-003**, 70 Fed. Reg. 7513 (Feb. 14, 2005), as amended at 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.

NUOFDC system users will have the ability to 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 a living individual involved in the incident. Audit logs and user contact information may be retrieved by username or other personal identifier of a system user.