United States Department of Justice
Justice Management Division

Privacy Impact Assessment
for the
National Law Enforcement Accountability Database
(NLEAD) System

Issued by:
Morton J. Posner
JMD Senior Component Official for Privacy

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

Date approved: December 7, 2023

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

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

On May 25, 2022, the President issued Executive Order 14074, *Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety* (the "Executive Order"). Section 5 of the Executive Order directs the Attorney General to establish a National Law Enforcement Accountability Database ("NLEAD") for official records documenting instances of law enforcement officer ("LEO") misconduct, commendations, and awards. The Executive Order strives to further accountability and transparency through improved LEO hiring and background investigations.

Consistent with the Executive Order, the Department of Justice has established the NLEAD system to facilitate a process of strengthened hiring practices and background investigations while protecting the safety, privacy, and due process rights of LEOs identified in the NLEAD. The NLEAD will operate using a pointer system, a database management model which utilizes a "pointer" to indicate that a record of a particular type exists for a searched individual and points the requester to the location of the record (i.e., the source agency). As specified by the Executive Order, the NLEAD will include data indicating that records exist for the following categories related to officer misconduct: criminal convictions; suspensions of a LEO's enforcement authorities, such as de-certification; terminations; civil judgments, including amounts (if publicly available), related to official duties; resignations or retirements while under investigation for serious misconduct; and sustained complaints or records of disciplinary action based on findings of serious misconduct. Officer commendations and awards are included only when one of these other categories of information is identified in the NLEAD. The NLEAD will be used, as appropriate and consistent with applicable law, in connection with the hiring, job assignment, and promotion of federal LEOs, through connecting users who query NLEAD with the Federal Law Enforcement Agencies that maintain the underlying records detailing the misconduct, commendation, and awards.

This PIA covers only the NLEAD system and not the underlying records held by the source agency. The underlying records are covered by the source agencies' own privacy documentation (e.g., System of Records Notice and PIA), as appropriate.

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.

As noted above, the NLEAD will operate as a pointer system, with the Department of Justice only maintaining a centralized, searchable database management system containing limited personally

identifiable information (PII) (*i.e.*, name, date of birth, and a unique hash of the social security number (SSN)[1], and last four digits of the SSN) of applicable federal LEOs. The purpose of the pointer system is to refer law enforcement agencies conducting background checks to the source agencies with the underlying records pertaining to those categories of information in the Executive Order. The NLEAD is intended to ensure relevant, timely, complete, and accurate information is considered in the LEO hiring, job assignment, and promotion process.

All information maintained in the NLEAD will be appropriately safeguarded and will only be used for authorized purposes. During the hiring process, the NLEAD will be queried by an authorized user[2] during the security screening and background investigation process (after a conditional offer of employment is made) by entering the SSN and DOB of a federal LEO applicant. The NLEAD will return a result that displays either (1) no responsive record, or (2) information on one or more incidents of misconduct pertaining to the individual. For each misconduct incident, the information provided will include the date and type of the incident (e.g., criminal conviction, termination, civil judgment, etc.). When misconduct information exists in the NLEAD, the NLEAD will also include any agency or component-level commendations or awards, specifically, the date and type of each award.

To facilitate and expedite the connection of the requestor with the substantive underlying records, the NLEAD will display the contact information for the federal law enforcement agency that is the source of the information and maintains the underlying records. The underlying records will remain at the record-owning agency, while the Department of Justice will collect and maintain only the information necessary to direct an authorized user back to the originating agency when responsive records exist for the applicant.

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

Authority	Citation/Reference
Statute	5 U.S.C. 3301
Executive Orders	Executive Order 13764, *Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 To Modernize the Executive Branch-Wide Governance Structure and Process for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters*; and Executive Order 14074, *Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety*

[1] A unique hash for a SSN involves using a mathematical method to convert the recognizable and usable value of a SSN to an alternative numeric representation that can only be deciphered with a protected reverse mathematical process, i.e., a hash algorithm.

[2] Only authorized users and system administrators in designated roles will have access to the NLEAD. Authorized users will be from a federal law enforcement agency or vetting agency such as the Defense Department's Counterintelligence and Security Agency (DCSA). Authorized users and system administrators are required to use their federal accounts (.gov, .mil, etc.) and Personal Identity Verification (PIV) Card/Common Access Card (CAC) to access the NLEAD.

Federal regulation	
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

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

(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 and C	Legal names of current and former federal LEOs entered into the NLEAD
Date of birth or age	X	A, B and C	Dates of birth of current and former federal LEOs entered into the NLEAD
Place of birth			
Gender			
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B and C	A unique hash of the full social security numbers and the last four numbers of current and former federal LEOs entered into the NLEAD
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			

(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
Vehicle identifiers			
Personal mailing address			
Personal e-mail address			
Personal phone number			
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information	X	A, B and C	Records reflecting federal LEO resignations or retirements while under investigation for serious misconduct; records reflecting debarment; records reflecting revocation of security clearance based on serious misconduct; records reflecting federal LEO disciplinary action based on findings of serious misconduct
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	A, B and C	Records reflecting federal LEO convictions
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B and C	Records reflecting civil judgments relating to misconduct of federal LEOs
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
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)**	X	A, B and C	Other information collected to implement the Executive Order such as the date of the incident and the duty station of the federal LEO
System admin/audit data:			
- **User ID**	X	A and B	Date/time of access of DOJ/Component Employees, Contractors, Detailees, and other Federal Government Personnel
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**	X	A and B	Date/time of access of DOJ/Component Employees, Contractors, Detailees, and other Federal Government Personnel
- **Queries run**	X	A and B	Queries run of DOJ/Component Employees, Contractors, Detailees, and other Federal Government Personnel
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			

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	
Phone		Email			
Other (specify):					

Government sources:					
Within the Component		Other DOJ Components	X	Other federal entities	X
State, local, tribal		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	JMD authorized NLEAD users and account and data managers can login to the NLEAD for the purpose of supporting users, conducting audits, troubleshooting issues, and other support-related duties.

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.**
DOJ Components			X	Authorized users within DOJ Components can login to the NLEAD to input, search, run a bulk query, or update data recorded in the NLEAD.
Federal entities			X	Authorized users within federal law enforcement agencies can login to the NLEAD to input, search, run a bulk query, or update data recorded in the NLEAD.
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

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.

Section 5(g)(i) of the Executive Order requires the Department of Justice to publish, on at least an annual basis, public reports that contain anonymized data from the NLEAD aggregated by law enforcement agency. These NLEAD reports will not contain any identifying information and will be produced "in a manner that does not jeopardize law enforcement officer anonymity due to the size of the agency or other factors."

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

The NLEAD does not collect information directly from individuals. In addition to the generalized notice provided by the SORN, JUSTICE/DOJ-022, National Law Enforcement Accountability Database, 88 Fed. Reg. 83966 (12-1-2023), available at https://www.govinfo.gov/content/pkg/FR-2023-12-01/pdf/2023-26073.pdf, each federal law enforcement agency will provide an approved notice of the NLEAD to its LEOs. For current employees, notice and a list of Frequently Asked Questions will be distributed by the component. The Department of Justice will also maintain a public-facing NLEAD website, which will include specific information about the NLEAD, as well as a link to the SORN.

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

The NLEAD does not collect information directly from individuals, and therefore cannot provide for the voluntary collection, use, or dissemination of information in the system.

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.

A request for access to information in the NLEAD can be made under FOIA and/or the Privacy Act procedures outlined in Subpart D, Part 16, Title 28, Code of Federal Regulations. Notice of these procedures are specified in the Record Access Procedures section of the SORN, JUSTICE/DOJ-022, National Law Enforcement Accountability Database, 88 Fed. Reg. 83966 (12-1-2023), available at https://www.govinfo.gov/content/pkg/FR-2023-12-01/pdf/2023-26073.pdf. Because the underlying records will remain with the source agencies, there will be coordination between the NLEAD administrators and responsible officials at the source agencies with respect to access and correction requests by individuals whose records are contained in the NLEAD.

Section 6: Maintenance of Privacy and Security Controls

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

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** ATO issued on November 28, 2023. **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:**

	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** The NLEAD is classified as FIPS High based on the nature of the data types it contains.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** See 6.2, below.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** The NLEAD application data input and modifications can be tracked through database logging and auditing functions. Audit logs are designed to be checked by system administrators on at least a weekly basis. Access and changes to the NLEAD data are captured in audit logs that are assigned to the Justice Security Operations Center and security professionals via Splunk[3] with appropriate system roles to monitor the audit logs. See 6.2, below.
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:** No additional training is required to use the NLEAD.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

The NLEAD is a web-based application hosted on a FedRAMP-certified cloud platform, which is a

[3] The Department's iteration of Splunk captures, indexes, and correlates "real-time" event data in a searchable repository from which IT and information security staff can generate graphs, reports, alerts, dashboards, and visualizations of various events. The Splunk solution provides insight into operational, security, and functional aspects of the environment. Splunk is covered under separate privacy documentation.

fully Certified and Accredited (C&A) production environment according to generally accepted standards and guidelines for C&A Department of Justice systems and networks.

Information in the NLEAD will be safeguarded in accordance with appropriate laws, rules, and policies, including the Department of Justice's automated systems security and access policies and Interconnection Security Agreements with interagency subscribers. All PII will be encrypted in accordance with applicable NIST standards when transferred between the Department of Justice and a subscriber agency. Record-owning agencies are only permitted to share information with the NLEAD using encrypted file sharing through the Department of Justice network. The NLEAD technical team follows a process to intake and validate data prior to submission in the NLEAD system to ensure that it meets the technical and system requirements. The process involves the review of the submitted data for data quality and the presence of all necessary data elements prior to it being uploaded in the NLEAD. Any check that is not passed is returned in an error file to the originating agency for correction prior to inclusion in the NLEAD.

Direct access to the NLEAD will require authorized users to login using PIV/CAC cards. Access to information in the NLEAD will be strictly limited to authorized users and system administrators (Department of Justice personnel and contractors) who have access to the Department of Justice's network and an official need for access to perform their duties. The type of data accessible to users in the NLEAD will be restricted by user classification designated by user roles and privileges. The NLEAD system administrators will set the necessary and appropriate account management functions and security settings for each user. Only the NLEAD system administrators can create, update, enable, and disable user accounts. The NLEAD system administrators will ensure that the certification agent or their delegee validates system security at least annually and will also make computers available for periodic reviews of the security configuration by independent testers.

The Department of Justice will ensure that NLEAD personnel have access to, are aware of, and comply with all Department of Justice policies, guidelines, and procedures (DOJ Order 2640.2 (series), DOJ IT Security Standards) related to the use of Department of Justice information technology resources.

Any modification to data input in the NLEAD can be tracked through database logging and auditing functions. System administrators will review audit logs on at least a weekly basis. The Justice Security Operations Center and Department of Justice security professionals also monitor the audit logs via Splunk for any access or data modifications.

All authorized users must accept the NLEAD rules of behavior, which includes the proper handling of sensitive system data for Unclassified//For Official Use Only, regardless of whether it is in electronic or hardcopy form.

By Department order, all Department of Justice users with access to Department networks, including the NLEAD, must receive an annual Cyber Security Assessment Training, which includes information on certain federal information privacy laws, such as the Privacy Act, and requirements for proper handling of PII. The training identifies potential risks and vulnerabilities associated with using Department of Justice-owned IT systems, provides a review of the user's role in protecting these systems, and establishes guidelines to follow at work and in mobile settings to protect against attacks on IT systems.

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 Department of Justice is working with the National Archives and Records Administration to create a records retention and disposal schedule for records in the NLEAD.

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:

JUSTICE/DOJ-022, National Law Enforcement Accountability Database, 88 Fed. Reg. 83966 (12-1-2023), available at https://www.govinfo.gov/content/pkg/FR-2023-12-01/pdf/2023-26073.pdf.

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.***

Data Collection, Sources, and Maintenance of the Information

The NLEAD system will collect and maintain sensitive information about LEOs, which necessitates safeguards to ensure proper handling. Information in the NLEAD will be safeguarded in accordance with appropriate laws, rules, and policies, including the Department of Justice's automated systems security and access policies and Interconnection Security Agreements with interagency subscribers. All PII will be encrypted in accordance with applicable NIST standards when transferred between the

Department of Justice and a source agency. Additionally, rather than simply identifying an individual by name, which could be less than unique, the Department of Justice will use unique hashes linked to an individual's SSN to assure that the NLEAD information attributed to an individual is, in fact, intended to apply to that specific individual. For record-owning/subscribing agencies to share information with the NLEAD, they must use encrypted file sharing through the Department of Justice network. The NLEAD technical team validates data prior to submission in the NLEAD system to ensure that it meets the technical and system requirements.

Access Controls
Direct access to the NLEAD will require authorized users to login through DOJLogin (Okta)[4] with PIV/CAC cards, which meets the NIST Authenticator Assurance Level 3 (AAL3) standards.[5] Access to information in the NLEAD will be strictly limited to authorized users and system administrators (Department of Justice personnel and contractors) who have access to the Department of Justice's network and an official need for access to perform their duties. The type of data accessible to users in the NLEAD will be restricted by user classification designated by user roles and privileges. The NLEAD system administrators will set the necessary and appropriate account management functions and security settings for each user. Only NLEAD system administrators can create, update, enable, and disable user accounts. To perform these functions, the system administrators must be identified and profiled for such privileges in the NLEAD application by the Department of Justice's technical service provider. The NLEAD system administrators will ensure that the certification agent or their designee validates system security at least annually and will also make computers available for periodic reviews of the security configuration by independent testers.

Mitigating the Risk of Collecting/Maintaining Inaccurate Information
The NLEAD is designed to collect only the PII necessary to identify an individual and direct the requester back to the agency that houses the underlying records. Rather than collecting the underlying misconduct records themselves, which would significantly increase privacy risks, the NLEAD will operate as a pointer system, directing the requester to the source agency for underlying records. This serves to mitigate the risk of the NLEAD collecting and maintaining inaccurate information about a LEO. The security personnel conducting the NLEAD check will be required to verify the information in the NLEAD with the source agency before making any decisions involving the applicant.

The Department of Justice team handling incoming NLEAD data validates the data coming in and seeks clarification from the source agency regarding any inconsistencies. This process includes the secure transfer of files from source federal law enforcement agencies, review of the data by data managers, and clarification/resolution of any discrepancies.

Further, the NLEAD requires source agencies to provide quarterly data updates; however, source agencies may contact the Department of Justice's NLEAD team at any time to update records

---

[4] DOJLogin (Okta) provides a mechanism to use multifactor authentication methods for users, using an enterprise-grade, identity management service that enables DOJ to manage users' access to applications or devices. Okta runs in the cloud on a secure platform, which integrates with on-premises applications, directories, and identity management systems. Additional information is available at: https://www.okta.com/products/. Okta is covered under separate privacy documentation.

[5] NIST Special Publication 800-63B sets forth the requirements for AAL3, the highest level of authentication. See NIST Special Publication 800-63B for more information.

pertaining to a LEO.

Risk of Unauthorized Disclosure

In order to prevent unauthorized disclosure of NLEAD data, access to the NLEAD is strictly limited to authorized users only with approved usage and privileges, as assigned. Additionally, the NLEAD data is only accessible to authorized users who are able to provide the correct name, date of birth, and complete SSN of a LEO. This creates an additional level of security to ensure that authorized users have a legitimate and official need to access the information of the LEO queried. Further, as discussed above, the NLEAD pointer system serves to mitigate the risk of unauthorized disclosure of substantive information about a LEO, as all underlying records remain with the source agency.