Federal Bureau of Investigation

Privacy Impact Assessment
for the
Next Generation Identification Biometric Interoperability

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

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

Date approved: April 23, 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.)

This Privacy Impact Assessment (PIA) is an update to the Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Biometric Interoperability PIA published in January 2012.[1] Since that time, the NGI System has replaced IAFIS as the FBI's biometric and criminal history records system.[2] The NGI System is managed by the Criminal Justice Information Services (CJIS) Division of the FBI. The NGI System is interoperable with the Department of Homeland Security (DHS) Automated Biometric Identification System, known as IDENT,[3] and the Department of Defense (DoD) Automated Biometric Identification System, known as ABIS. Biometric interoperability permits the FBI, DHS, and DoD to share relevant and essential identity information in an automated and timely manner. Interoperability between the federal agencies is conducted in compliance with memoranda of understanding, technical agreements, and legal and policy requirements. This PIA addresses risks of biometric interoperability from the perspective of the FBI; the DHS and DoD conduct separate privacy documentation, as appropriate, regarding biometric interoperability addressing risks from the perspective of those agencies.

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.

In the wake of the terrorist attacks of September 11, 2001, biometric interoperability between the FBI, DHS, and DoD began to be implemented in accordance with federal law and policyin order to enable the rapid and automated sharing of biometric identification data, as well as related biographic, criminal history, national security, immigration, and military force protection information to meet the respective agencies' missions. Biometric data increases the accuracy and reliability of identification systems, thereby reducing the risks to individuals of misidentification when the government accesses personally identifying information for a law enforcement or national security purpose. By contrast, identification systems that rely on less reliable associational information such as names or social security numbers, are subject to much greater risk of inaccuracy, as well as fraud or other forms of manipulation, placing innocent individuals needlessly at risk.

The categories of fingerprints currently maintained in the NGI System include: persons fingerprinted

---

[1] See www.fbi.gov/how-we-can-help-you/need-an-fbi-service-or-more-information/freedom-of-informationprivacy-act/department-of-justice-fbi-privacy-impact-assessments

[2] See NGI System of Records Notice, 84 Fed. Reg. 54,182 (October 9, 2019)

[3] IDENT will be replaced by the Homeland Advanced Recognition Technology (HART) system in the near future; however, all interoperability functions will remain the same.

as a result of arrest, incarceration, or other authorized criminal justice purpose; persons fingerprinted for employment, licensing, or other authorized noncriminal justice purpose, such as federal background checks and military service; persons fingerprinted for visa, alien registration, immigration, naturalization, or related purposes; and individuals fingerprinted for authorized national security purposes (including known or suspected terrorists and military detainees). The NGI System also contains additional biometrics associated with the ten-print fingerprints, such as palm prints, photos, and iris images.

The IDENT system is used by DHS for storage and processing of biometric and associated biographic information for the purposes of homeland security, law enforcement, immigration, and other DHS mission-related functions. The data maintained in IDENT is provided by DHS components, including United States (U.S.) Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), and the Transportation Security Administration (TSA). The IDENT system also maintains biometric and relevant biographic data collected from visa applicants for the Biometric Visa Program which is managed by the U.S. Department of State (DOS) Consular Affairs.

The ABIS system is used by DoD for storing, matching, and sharing biometric and associated biographic information collected in support of DoD operations. The data maintained in ABIS is provided by DoD components, including U.S. Military Services (e.g., Marine Corps) and U.S. Combatant Commands.

DHS and DoD privacy impact assessments can be found at: https://www.dhs.gov/topics/privacy and https://dpcld.defense.gov/Privacy.aspx.

NGI/IDENT interoperability:

(a) The NGI System to IDENT

Criminal justice fingerprints searched or maintained in the NGI System include fingerprints of individuals encountered by law enforcement as a result of a criminal inquiry, a lawful detention, arrest, or incarceration. These criminal justice fingerprints are submitted to the NGI System by federal, state, local, tribal, and territorial agencies.[4] After the NGI system has been successfully queried for these fingerprints , the IDENT system is also automatically queried for them as well. Criminal justice fingerprints account for the majority of the fingerprint transactions shared with IDENT for a biometric search. In addition to the fingerprints, the name, date of birth, and gender of the subject are sent to IDENT, as well as the Originating Agency Identifier (ORI)[5], and the Univeral Control Number (UCN)[6]. Unless there is a match, the NGI data is not retained by the IDENT system.

If there is an identity match in IDENT, it will return a response to the NGI System that contains name, date of birth, place of birth, gender, record identifier, and photo. This information is not retained in the NGI System, but the DHS Fingerprint Identification Number (FIN) is maintained on the NGI

[4] Foreign arrest fingerprints maintained by the FBI are sent manually, not automatically via the NGI System, to search IDENT.
[5] An ORI is a unique number identifying the authorized contributor of the biometric event to the NGI System.
[6] A UCN is a unique number assigned to each identity maintained in the NGI System.

System record to establish a pointer between the two systems for record linking purposes. In the event a "match" response is received from IDENT, the NGI System generates a separate query to a separate ICE system regarding the immigration status of the individual. After receiving both the IDENT match response and the ICE response, the NGI System generates a response to the original submitting criminal justice agency, if the state agency has installed a program to electronically receive this additional DHS information. In addition, if no fingerprint match is found in IDENT, but the subject appears to be a non-U.S. person based on the NGI System record, the NGI System sends a query to ICE. These queries are only generated for criminal arrests that have not matched in IDENT. ICE uses this process to identify subjects in law enforcement custody who may be appropriate for removal but who lack previous encounter information in IDENT.

If an NGI System search results in a match in IDENT and that system already maintains a separate, independent encounter with the individual, then a new encounter will be create in IDENT. The new encounter in IDENT includes a pointer within the record to alert IDENT users of another information source regarding that identity. The IDENT record does not maintain the criminal history information but retains the UCN and is updated with the subject's name, date of birth, gender, and fingerprint images. If there is not a match, no NGI System information is retained in IDENT.

In addition, certain non-criminal justice fingerprint transactions are sent from the NGI System to IDENT for a secondary biometric search. These transactions include individuals fingerprinted for federal employment background investigations and security clearances. Participating agencies include the Defense Counterintelligence and Security Agency (DCSA), the DOS Diplomatic Security (DS) Office of Personnel Security and Suitability (OPSS), and the International Criminal Police Organization. If there is an identity match in IDENT, it will return a response to the NGI System that contains name, date of birth, place of birth, gender, record identifier, and photo. This information is not retained in the NGI System. As with the criminal fingerprint submissions, after receiving the match response from IDENT, the NGI System generates a query to ICE to obtain the immigration status of the individual. After receiving both the IDENT match response and the ICE response, the NGI System combines the responses to send to the original agency, if the agency is programmed to receive the response.

DCSA transactions are only queries and no information is retained in IDENT, even when there is a match. DOS DS OPSS transactions are retained in IDENT regardless of an independent encounter and the IDENT record is updated with the subject's name, date of birth, gender, and fingerprint images. The UCN is not provided to IDENT for non-criminal justice fingerprint transactions. Finally, for humanitarian purposes, the fingerprints of unknown deceased persons are forwarded from the NGI System for a search of IDENT to assist in identifying human remains, victims of crimes such as homicide, or even persons who have been missing. The NGI System sends the combined IDENT and ICE response to the originating agency. The ability to search IDENT with unknown deceased fingerprints has aided in the successful identification of deceased victims in several cold cases.

The FBI shares certain data sets in bulk with DHS rather than sending transactions automatically via the NGI System to IDENT. These data sets include the wanted individuals/warrants and sex offender records from the National Crime Information Center (NCIC)[7] system and certain national security and

[7] NCIC is a criminal justice system maintained by the CJIS Division that has separate privacy documentation. Law

foreign fingerprints maintained in the NGI System. Because the NCIC system is name-based, to avoid the risk of misidentification, only those identities that have associated fingerprints in the NGI System are shared with IDENT. The wants/warrants and national security/foreign records shared in bulk with DHS are retained in IDENT regardless of whether IDENT has an independent encounter; DHS may only retain the sex offender records if IDENT has an independent encounter.

The NCIC wants/warrants are shared with IDENT every four hours, and the national security/foreign fingerprints and NCIC sex offender records are shared with IDENT once per day. In all instances, the fingerprints and basic identity elements (i.e., name, date of birth, place of birth) associated with the UCN are sent to IDENT. Consistent with NCIC policy, in order to reduce the risk of misidentification, DHS must independently confirm with the record owning law enforcement agency if a wanted individual or warrant has matched an identity in IDENT. When appropriate, record deletions are provided via an NGI System delete message to IDENT. An automated synchronization process between IDENT and the NGI System occurs the first of every month for the wants/warrants and the national security/foreign records, and a manual synchronization process occurs annually for the sex offender records.

(b) IDENT to the NGI System

DHS sends several types of fingerprint inquiries via IDENT to the NGI System, including DOS, USCIS, CBP, and ICE transactions. DHS components that use IDENT must affirmatively choose to search the NGI System. IDENT will not automatically send the transaction to the NGI System unless the user requests a separate search. As an agency with law enforcement components, DHS submits criminal justice fingerprints taken pursuant to arrest or other criminal justice purpose via IDENT to the NGI System for search or retention. If a match occurs in the NGI System, the criminal history information and associated biographic information will be returned to DHS. Only the UCN is retained in IDENT to serve as a pointer to criminal history in the NGI System. IDENT is not programmed to retain the criminal history; however, IDENT returns the NGI System response and criminal history to the originating DHS component which may retain the information in its case management system. For those searches retained in the NGI System, identity information such as name, date of birth, gender, as well as fingerprint, photos, and iris images from IDENT are maintained.

DHS sends fingerprints to the NGI System collected by CBP at the nation's land, sea, and air borders to assist with admissibility determinations. The NGI System responses provide criminal history that may be relevant to admissibility or law enforcement action. In a program instituted at major airports, CBP sends fingerprints for a rapid search of the NGI System. These fingerprint searches are not retained in the NGI System. In these rapid search situations, the NGI System returns a candidate list to CBP, rather than a positive identification. If a returned candidate appears to be a match, CBP may subsequently send criminal inquiry fingerprints to the NGI System to obtain the subject's criminal history. If CBP arrests the subject, CBP would submit criminal retain fingerprints to the NGI System at that time.

The NGI System also searches and retains the DHS-collected fingerprints of subjects of interest in foreign countries, including those collected pursuant to ICE's Biometrics Identification Transnational Migration Alert Program (BITMAP). The BITMAP fingerprints, collected in partnership with foreign

---

enforcement users across the country query its files millions of times per day.

law enforcement, are of subjects who may pose a criminal or national security threat to the U.S. The BITMAP fingerprints may be submitted as retain or non-retain to the NGI System, depending upon the category assigned by ICE. For example, gang members and special interest aliens are submitted as retain but many other fingerprints are submitted as non-retain.

DHS also sends non-criminal justice fingerprint inquiries via IDENT to the NGI System, including fingerprint searches for the purpose of visa issuance. The DHS performs this service on behalf of the DOS's Consular Offices. The NGI System is capable of processing tens of thousands of visa fingerprint submissions per day with an expedited response time within 15 minutes. These DOS transactions are sent as search only and are not retained in the NGI System. In addition, the USCIS submits fingerprints of applicants for immigration benefits to the NGI System for criminal history background checks. These USCIS transactions are retained in the NGI System. As with the criminal justice submissions, if a match occurs in the NGI System, the criminal history information and associated biographic information will be returned to DHS but IDENT retains only the UCN. The originating DHS component may retain additional information.

NGI/ABIS interoperability:

(a) The NGI System to ABIS

The NGI System searches of ABIS are limited to those fingerprint transactions originating from the FBI and other federal agencies. Searches of ABIS are conducted at the same time as the NGI System search. The FBI queries ABIS with select national security, criminal, and humanitarian fingerprints. For example, the FBI's Mobile Biometric Application program allows FBI agents to collect ten-print fingerprints on mobile devices and to search those fingerprints in the NGI System, IDENT, and ABIS.[8] The DHS BITMAP queries sent to the NGI System are forwarded to ABIS for an additional search of the DoD holdings. The NGI System also forwards criminal and background check inquiries from agencies such as the DOS, the U.S. Marshals Service, and the Nuclear Regulatory Commission. In almost all instances, these fingerprint searches are not maintained in ABIS, and if there is a match, ABIS retains no information. For searches that are retained in ABIS, (typically queries of non-US persons) if the search results in a match, ABIS retains the name, date of birth, gender, and fingerprint images from the NGI System. Unlike IDENT, ABIS does not retain the UCN. When there is a fingerprint match to an ABIS record, identity information such as name, place of birth and date of birth, is returned to the contributing agency via the NGI System. The NGI System does not retain a pointer on transactions that match in ABIS.

(b) ABIS to the NGI System

The DoD forwards criminal and non-criminal justice fingerprints to the NGI System via ABIS from its military branches and military operations. The DoD also sends certain inquiries from the U.S. Coast Guard to search the NGI System and for a subsequent search of IDENT. When there is a match in the NGI System, the criminal history and associated biographic information are returned to DoD. The law enforcement components of DoD may submit arrest fingerprints via ABIS or may submit directly to the NGI System. DoD also sends the fingerprints of employees working on military bases outside of

[8] See www.fbi.gov/file-repository/pia-mobile-biometric-application.pdf/view

the U.S. for a background check. The majority of these employee fingerprints are non-U.S. persons. Background checks of military personnel are sent directly to the NGI System by the DCSA. For those searches retained in the NGI System, identity information such as name, date of birth, gender, as well as fingerprint, photos, and iris images from ABIS are maintained.

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	8 U.S.C. §1722; 28 U.S.C. §§ 533, 534; 42 U.S.C. § 3771; 44 U.S.C. § 3301; USA PATRIOT ACT of 2001, Pub. L. No. 107-56; Intelligence Reform and Terrorism Prevention Act, Pub. L. No. 108-458.
Executive Order	E.O. 8781, 8914, 10450, 13356
Federal regulation	28 CFR §§ 0.85, 20.31, 20.33
Agreement, memorandum of understanding, or other documented arrangement	DHS/FBI/DOS Improved Information Sharing Services MOU, July 2008; FBI/DoD MOU Governing Information Sharing, Operational Coordination, and Investigatory Responsibilities, August 2011
Other (summarize and provide copy of relevant portion)	HSPD 24/NSPD 59

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.

Both DHS and DoD may submit photos (i.e., face images, and scars, marks, and tattoos) and iris images with the ten-print fingerprint transactions sent to the NGI System. These additional biometrics are used to augment the retained identity records in the NGI System and may be used to perform face and iris recognition services. Separate PIAs regarding the NGI System's face and iris services have been published on the www.fbi.gov website.

(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	
Date of birth or age	X	A, B, C, and D	
Place of birth	X	A, B, C, and D	
Gender	X	A, B, C, and D	
Race, ethnicity, or citizenship	X	A, B, C, and D	
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, and D	
Tax Identification Number (TIN)			
Driver's license			
Alien registration number	X	A, B, C, and D	
Passport number			
Mother's maiden name			
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			
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, 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
Juvenile criminal records information	X	A, B, C, and D	
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			
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, and D	
- **Video containing biometric data**			
- **Fingerprints**	X	A, B, C, and D	
- **Palm prints**			
- **Iris image**	X	A, B, C, and D	
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**	X	A, B, C, and D	
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	
- **User passwords/codes**	X	A	
- **IP address**	X	A	
- **Date/time of access**	X	A	
- **Queries run**	X	A	
- **Contents of files**	X	A	
Other (please list the type of info and describe as completely as possible):	X	A, B, C, D	Unique identifying numbers (e.g., UCN, FIN)

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	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	X		
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				
DOJ Components				
Federal entities		X	X	Fingerprints and associated data are shared between FBI, DHS, and DoD with automated system connection/access; limited data sets are shared in bulk with DHS.
State, local, tribal gov't entities				

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.**
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.

The fingerprints maintained within the NGI System, including those submitted by DHS and DoD for retention, may be used for FBI research and development purposes in accordance with applicable federal law and regulations. The FBI has a longstanding relationship with the National Institute of Standards and Technology (NIST)[9] to perform biometric testing. When the FBI provides data to NIST, it is subject to strict security and use protections pursuant to an interagency agreement between the two agencies. Additional protections are delineated in "Government Furnished Information" letters which the FBI provides to NIST regarding specific research projects and data sets. Any fingerprints used for research and development would be sent without other associated PII; however, some non-unique biographic information such as year of birth and sex, as well as other biometrics may accompany the fingerprints if required by the specific research activity. The data is encrypted in accordance with Federal Information Processing Standards 140-2 requirements prior to release. The data is stored in FBI laboratories which have received an authority to operate in accordance with FBI security policy and the Federal Information Security Modernization Act. In addition, only those with documented authorization and a true need-to-know are granted access to the data. No fingerprints are released to the public for "open data" purposes.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the

[9] NIST, part of the Department of Commerce, is one of the nation's oldest physical science laboratories. Its core competencies include measurement science, rigorous traceability, and development and use of standards.

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.

No Privacy Act notice is provided to individuals regarding the collection, use, and sharing of their criminal or national security fingerprints in the NGI System. The FBI has been exempted from the requirement of 552a(e)(3) for the criminal and national security records maintained in the NGI System pursuant to the provisions of 552a(j) and (k) of the Act. A Privacy Act notice is provided to individuals when fingerprints are collected for retention in the NGI System for civil purposes, such as employment and licensing. This Privacy Act notice also is required for the non-criminal justice fingerprints submitted by DHS and DoD for search and retention in the NGI System. The NGI System's SORN provides general notice of the collection and use of fingerprints and the most current version may be found at 84 Fed. Reg. 54,182 (October 9, 2019). This PIA also provides general notice, as does the previously published PIAs regarding the NGI System, which may be found at https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments.

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.

An individual whosefingerprints are collected in connection with a criminal or national security investigation has no opportunity to refuse the collection of his or her biometrics. Nevertheless, federal agency criminal or national security uses of the information in the NGI System must comply with the provisions of applicable law, including the Privacy Act.. An individual submitting civil fingerprints, such as for employment, security clearance, or immigration benefits, voluntarily provides their fingerprints to obtain the relevant benefit, and receives a notice pursuant to 552a(e)(3) of the Privacy Act.

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.

As noted above, the FBI maintains exemptions from access and amendment provisions of the Privacy Act for certain records maintained in the NGI System. However, title 28 CFR part 16, subpart A, provides general guidance on access to information in FBI files pursuant to the Freedom of Information Act; and 28 CFR part 16, subpart D, provides general guidance regarding access to, and amendment of, information in FBI files to the extent it is available pursuant to the Privacy Act. In addition, title 28 CFR 16.30-16.34 establishes specific procedures for an individual to obtain a copy of his or her criminal history record from the NGI System for review and correction.

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):** January 9, 2023 to January 8, 2026. **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:** No POAMs related to privacy controls.
	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:** Confidentiality: high; Integrity: high; Availability: high / The NGI System is high across all categories on two grounds. The first is that law enforcement officer safety requires access to this information in a timely and accurate manner. The second is that public privacy requires confidentially be maintained to those members of the user community with need to know for this information.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The NGI System is continually monitored at the host and network layer. FISMA policy compliance testing occurs monthly.
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:** Host operating system logs are consolidated into the CJIS enterprise system audit consolidation and monitored for irregular activities or compliance failures. The NGI System Security Administrator reviews security-related logs on a weekly basis.
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:** Pursuant to the CJIS Security Policy, law enforcement users receive security/privacy training as an initial requirement of access to the NGI System, and annually thereafter.

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 primary transmission method of biometric submissions to the NGI System is electronically via the CJIS wide area network (WAN). The CJIS WAN is a telecommunications infrastructure that connects authorized agencies to the NGI System and other host computer systems. The CJIS WAN provides a secure transport mechanism that supports the exchange of encrypted biometric and criminal history record information. The CJIS WAN is configured by FBI personnel and secured through firewall mandates. Authorized external NGI System users connect to NGI System services via the Law Enforcement Enterprise Portal (LEEP)[10] interface, and authentication of these users occurs at the LEEP interface.

Fingerprint searches submitted from DHS and DoD are compliant with the Electronic Biometric Transmission Specifications (EBTS). The EBTS ensures compatibility with the NGI System and extends beyond the American National Standards Institute/National Institute of Standards and Technology - Information Technology Laboratory (ANSI/NIST-ITL) standard. ANSI/NIST-ITL is developed and maintained in conjunction with NIST and the biometric community. While the ANSI/NIST-ITL standard provides guidelines for the exchange of information between various local, state, tribal, federal, and international biometric systems, the EBTS defines requirements to which agencies must adhere when electronically communicating with the NGI System.

Only authorized criminal justice and national security agencies may search and retain fingerprints within the NGI System. The NGI System provides access and authentication to system level information based upon the authorized General User (contributor) and Privileged User (system administrator) access and as defined within the NGI System's User's Guide. Privileged Users are provided with capabilities to view submission data for purposes linked to administration of the NGI System. All General User and Privileged User actions are logged in the system audit logs with full traceability to individual users performing actions. All system audit logs are retained in accordance with FBI retention policies and guidelines. General Users of the NGI System and corresponding capabilities are controlled through agency agreements according to the CJIS Security Policy and vetted by the individual federal and state agency CJIS Systems Officers (CSOs).

DHS and DoD must ensure compliance with the CJIS Security Policy and applicable CJIS User Agreements. The CJIS Security Policy governs the information security requirements for all CJIS Systems, including the NGI System, and controls include security training, reporting of security incidents, access control, media protection, and physical and personnel security. The CJIS User Agreement specifies the ways in which each agency - CJIS and each user agency - is responsible for appropriate security measures as applicable to physical security of terminals and telecommunications lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security; dissemination and logging; and security of records. With the NGI System security requirements, dissemination of information is linked to the authorized agency

[10] LEEP is a federated gateway that securely connects law enforcement and national security users to systems via established secure connections. It is also managed by the CJIS Division and has separate privacy documentation.

that requested the information. The system stores information regarding dissemination, such as date, time, and requester in audit logs. Risks are also mitigated by training and by periodic audits conducted by the FBI to ensure system searches are relevant and necessary to the person's official duties.

The CJIS Division has an established Audit Unit that regularly reviews implementation of FBI requirements by agencies that are authorized to access the NGI System. The CJIS Division performs triennial audits of all CJIS system agencies (CSA), the agencies that are responsible for federal or state connections to the NGI System and whose CSOs are responsible for implementing compliance. The state or federal CSOs, in turn, conduct audits of their agencies on a triennial basis. The state or federal CSO is responsible for implementing and ensuring compliance with the CJIS Security Policy. The CJIS Division provides training assistance and up-to-date materials to each CSO and periodically issues informational letters to notify authorized users of administrative changes affecting the system. CSOs at the federal and state level are responsible for the role-based training, testing, and proficiency affirmation of authorized users within their respective state or federal agencies. All users must be trained within six months of employment and biennially re-tested hereafter. The CJIS Division and CSA audits confirm that only authorized agency personnel are accessing the NGI System for authorized purposes.

The audits assess and evaluate users' compliance with CJIS Division's technical security policies, regulations, and laws. Audit reports are typically prepared within a few months and deficiencies identified during audits are reported to the CJIS Division Advisory Policy Board (APB). The APB operates pursuant to the Federal Advisory Committees Act and is comprised of representatives from federal, tribal, state, and local criminal justice agencies who advise the FBI Director regarding CJIS Systems, such as the NGI System. System access may be terminated for improper access, use, or dissemination of system records.

The NGI System is not available to users unless there has been an application for, and assignment of an ORI. Each using entity may only access the types of information for the purposes that have been authorized for its ORI. Such access is strictly controlled and audited by the CJIS Division. Federal and state CSOs must apply to the CJIS Division for the assignment of ORIs and CJIS Division staff evaluates these requests to ensure the agency or entity meets the criteria for the specific type of ORI requested. The CJIS Division maintains an index of ORIs and logs each dissemination of identification records to the applicable ORI.

In addition, the NGI System's Information System Security Officer is responsible for ensuring that operational security is maintained on a day-to-day basis. Adherence to roles and rules is tested as part of the security certification and accreditation process. All FBI employee and contractor personnel must complete privacy training and annual information security training. The training addresses the roles and responsibilities of the users of FBI systems and raises awareness of the sensitivity of the information contained therein and how it must be handled to protect privacy and civil liberties.

In accordance with 28 U.S.C. §534, the FBI does not disclose information from the NGI System outside of the authorized receiving agency or related agencies. Although this is a separate statute from the Privacy Act of 1974, it provides specific controls on the dissemination of criminal history record information, including identification of authorized recipients and potential sanctions for unauthorized disclosures. These restrictions are, in turn, reflected in long-standing and extensive system security standards and operating policies applicable to all system users. In addition, authorized users must

comply with applicable security and privacy protocols addressed in the CJIS Security Policy.

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 retention of records in the NGI system is subject to the requirements of the Federal Records Act, administered by the National Archives and Records Administration (NARA). NARA has approved the destruction of fingerprint cards and associated information, including other biometrics, when criminal and civil subjects attain 110 years of age. The published NARA records schedule number is N1-065-10-16. NARA has determined automated FBI criminal history information and NGI System transaction logs are to be permanently retained. Biometrics and associated biographic information may be removed from the NGI System earlier than the standard NARA retention period pursuant to a request by the submitting agency or the order of a court of competent jurisdiction.

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:

The NGI SORN is published at 81 Fed. Reg. 27,284 (May 5, 2016); 82 Fed. Reg. 24151, 156 (May 25, 2017); 84 Fed. Reg. 54,182 (Oct. 9, 2019)

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.***

Pursuant to its statutory authorities, the FBI has collected, maintained, and exchanged biographic and biometric information for many decades. Therefore, the searching and retention of fingerprints from DHS and DoD and the release of biometrics and criminal history in response to those searches within the NGI System does not constitute a new collection type or collection purpose. Biometric interoperability between the FBI and its federal partners was mandated by Congress, and since that time, the agencies have developed an ongoing working relationship and infrastructure to ensure relevant and secure data sharing. An entire team of subject matter experts within the CJIS Division is assigned to work daily with DHS and DoD. The FBI requires the submission of ten-print fingerprints from DHS and DoD to ensure the most reliable identification. Unlike biometrics such as latent prints or face photos which produce only candidates, the FBI has relied on ten-print fingerprints as positive identification for almost a century. The FBI continuously tests and evaluates fingerprint services within the NGI System to ensure optimal accuracy and timely responses.

The risk of the NGI System information being used by unauthorized persons or for unauthorized purposes is greatly mitigated by significant technical and policy safeguards. The requirements for access and dissemination of NGI System data were described in Section 2 of this PIA, and many of the system safeguards were discussed in Section 6.2. Specific to biometric interoperability, the NGI System data is exchanged with trusted federal partners that are also subject to the Privacy Act, as well as other relevant federal laws and executive orders. The data sharing between the FBI and DHS and between the FBI and DoD is in accordance with Memoranda of Understanding (MOUs) and Interface Control Agreements (ICAs). The FBI and DHS currently exchange data pursuant to a 2008 MOU and a new MOU is nearing completion after several years of negotiation. The FBI and DoD currently exchange data pursuant to a 2011 MOU and an Annex to that MOU is currently being drafted specific to interoperability data sharing. Notably, the MOUs and ICAs ensure that only minimum, mission-relevant data is shared between the agencies, that third-party data sharing is restricted, and that records are linked between the systems to ensure timeliness and accuracy.

In addition, biometric interoperability data protection strategies regarding NGI System data were developed in 2006 at the request of the CJIS APB. These data protection strategies undergo review every three years and are currently being revised in coordination between the CJIS Division and the CJIS APB. These strategies were implemented to ensure that the FBI maintained oversight and security of the NGI System data shared with DHS and DoD, as the NGI System is comprised mostly of state and local data. These protection strategies include informing all criminal justice partners of the status of interoperability; ensuring data in the federal systems are synchronized, current, and accurate; sharing/maintaining only data that is necessary to an agency's mission; and audit compliance with privacy and security requirements.

As discussed above, the agencies, types of data, and uses for the data are clearly defined and strictly regulated. The FBI takes action to correct any erroneous information of which it may become aware and has established policies and technical safeguards to both prevent inaccurate or unauthorized information from entering the NGI System and to conduct ongoing reviews of the information residing in the system. Additionally, the maintenance and dissemination of information by the FBI, DHS, and DoD must comply with the provisions of any applicable law, regulation, or policy, including the Privacy Act of 1974. Privacy risks are further reduced to the extent that agencies that contribute

information to the NGI System also have processes in place for access to or correction of their source records.