

# Federal Bureau of Investigation



## **Privacy Impact Assessment** for the Next Generation Identification Latent Services

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: March 10, 2022

*(May 2019 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 Next Generation Identification (NGI) Palm Print and Latent Fingerprint Files PIA published in January 2015. This PIA will provide updated information regarding latent services within the NGI System, which is managed by the FBI's Criminal Justice Information Services (CJIS) Division. The NGI System's latent services were designed to assist the FBI's law enforcement and national security partners in solving crime and protecting our nation against acts of terrorism. The NGI System is a national repository of biometrics (e.g., fingerprints, palm prints, face images, iris images) and any associated criminal history information.<sup>1</sup> This PIA only addresses the latent fingerprints and palm prints in the NGI System; the FBI has published separate PIAs for other biometrics and services in the NGI System.

Authorized law enforcement and national security agencies may be permitted to search latent prints obtained from evidence or during investigations against NGI System's criminal, civil, and national security biometric repositories. The NGI System also provides its authorized users with the ability to search latent prints against other unidentified latent prints retained within its Unsolved Latent File (ULF) and to enroll their unidentified latent prints into the ULF. In addition, newly submitted biometric events are searched against latent prints retained within the ULF of the NGI System.

## **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.*

Latent services within the NGI System provide law enforcement and national security partners with the ability to identify latent prints obtained from evidence within criminal and terrorism investigations. A latent print is a transferred impression of friction ridge detail (i.e., the raised portion of the epidermis of the palm and fingers) that is not readily visible. The identification of these latent prints provides new investigative leads to assist with solving crimes and/or intercepting terror plots against our nation, as well as protecting military personnel and coalition forces operating worldwide. These services also provide the ability to identify unknown deceased persons and eliminate individuals as persons of interest within active law enforcement investigations, clearing the innocent of suspicion, while helping to insure the guilty are held accountable.

The NGI System uses an automated algorithm that compares the unique characteristics of latent prints to retained biometrics. The FBI collaborates with the National Institute of Standards and Technology

---

<sup>1</sup> See NGI System of Records Notice, 81 Fed. Reg. 27,284 (May 5, 2016); 84 Fed. Reg. 54,182 (October 9, 2019).

(NIST)<sup>2</sup> to ensure that its biometric technology is of the highest standard.<sup>3</sup> Because latent technology continuously improves and advances, the FBI performs recurring standardized testing of latent print algorithms. The FBI deployed improved latent matching algorithms in May 2013, January 2018, and continues to collaborate with NIST to perform ongoing testing of latent print algorithms.

The NGI system provides the ability to search unidentified latent prints against a national repository of retained biometric identities, consisting of criminal, civil, and national security biometric identities, as well as other unidentified latent prints retained within the ULF. The criminal repository contains biometrics collected in proceedings related to the violation of criminal law, such as pursuant to arrest, detention, and incarceration. The civil repository contains biometrics collected for purposes such as employment, licensing, background checks, immigration benefits, military service, and security clearances, collectively “civil biometrics.” The national security repository contains the biometrics of known or suspected terrorists, and those obtained from foreign governments, federal partners, and others associated with the FBI’s authority to investigate national security threats. The ULF contains latent prints that have been searched against the NGI System but remain unidentified.

All civil biometric events submitted for retention within the NGI System are searched against the ULF; however, some civil biometrics are submitted for search, but not retention within the NGI System. In these instances, the submitting agency must affirmatively permit latent searching of its non-retained civil biometrics. At this time, the majority of non-retained civil biometric events are permitted to be searched against the ULF. In addition, if non-retained civil biometric events match to a criminal or national security identity in the NGI System, then the biometrics will be searched and disseminated accordingly.

The law enforcement agency searching latent prints against the NGI System has the option to designate which biometric repositories are to be searched. If no repository is designated, then only the criminal repository is searched by the NGI System. The submitter may also choose the number of candidates (i.e. “potential matches”) returned from a latent search, from one to ninety-nine. If no choice is made, a default of twenty candidates will be returned to the owner of the latent prints. The candidates are returned “lights out” from the NGI System to the latent print owner, meaning that there is no manual or human intervention at that time. The candidates returned from the NGI System include biometric and biographic information associated with the biometric identity.

Latent services within the NGI System are considered investigative leads; therefore, candidates require subsequent review by latent print examiners within the receiving law enforcement or national security agency to determine a positive identification. The NGI System also provides the ability for law enforcement and national security partners to request additional retained biometric events from the same identity if needed for comparison purposes. If upon comparing these candidates the latent prints remain unidentified, the latent print owner has the option to retain the biometrics in the ULF.

The ULF consists of nearly one million unidentified latent prints submitted by law enforcement and national security agencies where the latent prints are subject to ongoing searches by newly submitted criminal, civil, and national security biometrics to the NGI System. These searches may continue to

---

<sup>2</sup> 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.

<sup>3</sup> See <https://www.nist.gov/programs-projects/nist-evaluation-latent-fingerprint-technologies-elft>.

produce new candidates after the initial search and enrollment of the latent prints into the ULF. If a viable candidate is produced, the NGI System provides an automated notification to the owner of the latent prints. This notification includes such information as the biometrics, limited biographic information, and information necessary to contact the contributing agency of the biometric event. If the latent prints are subsequently identified following comparison by a latent print examiner, the owner of the latent prints may contact the owner of the matched biometrics for investigative purposes. The NGI System also supports the search of latent prints against the ULF, which produces new leads within unsolved cases. Candidates produced from the ULF are returned to the agency submitting the latent print search. If an identification is made and notification is provided to the NGI System, an automated notification is provided to the owner of the corresponding latent prints. This exchange of information may produce new leads within the unsolved investigations.

Law enforcement and national security partners have the option of providing their latent print comparison decisions to the CJIS Division to assist with analysis and enhancement of the latent matching algorithm within the NGI System. Latent prints that have been subsequently identified, and those associated with cases that are no longer actionable or have exceeded the statute of limitations, should be deleted from the ULF. The latent print owners may delete latent prints from the ULF electronically and the CJIS Division provides inventories and offers bulk delete services to the latent print owners. These actions ensure proper maintenance of the ULF and enhance its accuracy and timeliness. If the ULF reaches maximum capacity, the NGI System automatically deletes the oldest record and provides notification to the latent print owner. The owner has the option to re-enroll the latent prints if necessary.

Limited information is collected by the NGI System for a latent search or for enrollment into the ULF, as the latent prints are from unknown identities and include no other personally identifiable information (PII). Only the biometric itself is submitted to and searched within the NGI System. Other than information necessary for system verification and access authorization purposes, the information collected is primarily specific to the unique characteristics of the unidentified latent print, such as the friction ridge position and pattern type, if known or visible. In very limited instances, the submitters may include additional information such as place of birth, age range, sex, and race. This information is typically provided when the latent prints are obtained from unidentified deceased persons, as such information may be visible or available in those circumstances.

After the terrorist attacks of September 11, 2001, the FBI recognized the need to search its latent prints against other federal biometric systems. The Department of Homeland Security (DHS), the Department of Defense (DoD), and other national security and law enforcement partners submit their latent prints for search and enrollment in the NGI System as described above. If FBI latent prints remain unidentified after searching the NGI System and are enrolled into the ULF, they can be subsequently searched against the DHS Automated Biometric Identification System (IDENT) and the DoD Automated Biometric Identification System. These sharing efforts allow for latent prints maintained by the FBI, DHS, DoD, and other national security partners to be searched against participating biometric systems and to be retained within their respective unsolved latent files if the prints remain unidentified. Those latent prints identified by the other federal agencies are reported to the CJIS Division for notification to the latent print owners. The CJIS Division also shares the DoD's latent prints retained within the ULF with DHS.

The NGI System also provides the ability for law enforcement to search latent prints against participating external biometric systems. This capability is currently limited to latent searches transmitted by the Texas Department of Public Safety (TX-DPS) to the DHS for searches of IDENT. Currently, the TX-DPS has the ability to search latent prints against NGI and/or IDENT Systems. Latent searches designated for DHS are transmitted via the CJIS Wide Area Network (WAN), a secure telecommunications infrastructure, and include a repository indicator for routing purposes. The IDENT System produces a list of up to twenty viable candidates that are returned to the TX-DPS via the CJIS WAN. If any of the returned candidates result in a positive identification, the TX-DPS provides notification to DHS to obtain additional biographic information needed for investigative purposes. All latent prints that remain unidentified after searching the IDENT System may be retained within the ULF. The TX-DPS provides notification to DHS of all persons prosecuted or cleared as a result of identifications effected within the IDENT System. The DHS deletes all identified latent prints from the IDENT System within five days of notification from the TX-DPS.

The FBI's Preventing and Combating Serious Crime (PCSC) Program<sup>4</sup> and other authorized agreements support the exchange of biometrics between foreign countries and the United States for persons of interest within specific criminal and terrorism investigations. Currently, some foreign partners have modified access to latent investigative services within the NGI System, which allows for the search and return of only criminal identities. Unidentified latent prints owned by the FBI and having a nexus to terrorism are shared with some foreign partners for searches of their biometric systems, and subsequent unidentified latent prints are provided on a recurring basis. The files are extracted from the ULF of the NGI System and are uploaded into an Enterprise File Transfer Service for download purposes. All resulting latent print identifications are reported to the FBI for intelligence analysis and vetting of those posing a threat to national security.

**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	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	
Other (summarize and provide copy of relevant portion)	

---

<sup>4</sup> The PCSC Program permits the United States and its partner countries to cooperatively exchange biometric and biographic data to prevent and combat serious crime and terrorism. The Department of Justice is the signatory for the PCSC agreements; the FBI CJIS Division has been delegated the responsibility to implement the agreements.

### **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.***

As previously stated, limited personal information is included with latent print searches of the NGI System as the biometric is of an unknown identity. In reference to the table below, latent searches generally include only the unknown biometric image. However, the search may include age range, sex, race, height, weight, eye color, hair color, scars, marks, and tattoos. These additional descriptors are typically included when available to assist in identifying unknown decedents in which decomposition has significantly degraded biometric quality.

In response to latent searches, the NGI System returns viable candidates and their corresponding biometric images, names, and the unique numeric identifier of each. Also, as previously stated, law enforcement and national security partners have the option to retain unidentified latent prints within the ULF. If retained, the information included as part of the initial search is maintained and referenced for subsequent search purposes. Candidates produced from searches of the ULF include information beyond those returned within the initial candidate list. The PII returned within these notifications are noted within the table below.

Department of Justice Privacy Impact Assessment  
 FBI/Latent Services

(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
<i>Example: Personal email address</i>	X	<i>B, C and D</i>	<i>Email addresses of members of the public (US and non-USPERs)</i>
<b>Name</b>	X	A, B, C, and D	May also include local, state, and tribal law enforcement personnel if authorized to retain and/or search biometrics within the NGI System.
<b>Date of birth or age</b>	X	A, B, C, and D	See above.
<b>Place of birth</b>	X	A, B, C, and D	See above.
<b>Gender</b>	X	A, B, C, and D	See above.
<b>Race, ethnicity, or citizenship</b>	X	A, B, C, and D	See above.
<b>Religion</b>			
<b>Social Security Number (full, last 4 digits or otherwise truncated)</b>			
<b>Tax Identification Number (TIN)</b>			
<b>Driver's license</b>			
<b>Alien registration number</b>			
<b>Passport number</b>			
<b>Mother's maiden name</b>			
<b>Vehicle identifiers</b>			
<b>Personal mailing address</b>			
<b>Personal e-mail address</b>			
<b>Personal phone number</b>			
<b>Medical records number</b>			
<b>Medical notes or other medical or health information</b>			
<b>Financial account information</b>			
<b>Applicant information</b>			
<b>Education records</b>			
<b>Military status or other information</b>			
<b>Employment status, history, or similar information</b>			
<b>Employment performance ratings or other performance information, e.g., performance improvement plan</b>			
<b>Certificates</b>			
<b>Legal documents</b>			

Department of Justice Privacy Impact Assessment  
 FBI/Latent Services

(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
<b>Device identifiers, e.g., mobile devices</b>	X	A and B	May also be included within latent transactions submitted by local, state, and tribal law enforcement agencies.
<b>Web uniform resource locator(s)</b>			
<b>Foreign activities</b>			
<b>Criminal records information, e.g., criminal history, arrests, criminal charges</b>			
<b>Juvenile criminal records information</b>			
<b>Civil law enforcement information, e.g., allegations of civil law violations</b>			
<b>Whistleblower, e.g., tip, complaint, or referral</b>			
<b>Grand jury information</b>			
<b>Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information</b>			
<b>Procurement/contracting records</b>			
<b>Proprietary or business information</b>			
<b>Location information, including continuous or intermittent location tracking capabilities</b>			
<i>Biometric data:</i>			
<b>- Photographs or photographic identifiers</b>			
<b>- Video containing biometric data</b>			
<b>- Fingerprints</b>	X	A, B, C, and D	See above.
<b>- Palm prints</b>	X	A, B, C, and D	See above.
<b>- Iris image</b>			
<b>- Dental profile</b>			
<b>- Voice recording/signatures</b>			
<b>- Scars, marks, tattoos</b>	X	A, B, C, and D	See above.
<b>- Vascular scan, e.g., palm or finger vein biometric data</b>			
<b>- DNA profiles</b>			
<b>- Other (specify)</b>			
<i>System admin/audit data:</i>			
<b>- User ID</b>	X	A	
<b>- User passwords/codes</b>			
<b>- IP address</b>	X	A	
<b>- Date/time of access</b>	X	A	

Department of Justice Privacy Impact Assessment  
 FBI/Latent Services

(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
- <b>Queries run</b>	X	A	
- <b>Content of files accessed/reviewed</b>	X	A	
- <b>Contents of files</b>	X	A	
<b>Other (please list the type of info and describe as completely as possible):</b>			

Additionally, the Originating Agency Identifier (ORI) and/or Controlling Agency Identifier (CRI) may be returned in response to searches of the ULF. The ORI and CRI are unique numbers that correspond with the authorized contributor of the biometric event and are provided to law enforcement for subsequent communication should the submitted biometric result in a positive identification to latent print evidence.

Please note authorized law enforcement agencies may perform secondary queries of the NGI System to obtain associated criminal history information and additional biometric images after effecting a latent print identification. However, this information is not returned within the initial responses to the searches of latent prints via the NGI System.

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

<b>Directly from the individual to whom the information pertains:</b>				
In person		Hard copy: mail/fax		Online
Phone		Email		
Other (specify):				

<b>Government sources:</b>				
Within the Component	X	Other DOJ Components	X	Online
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):				

<b>Non-government sources:</b>			
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			Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.
	Case-by-Case	Bulk Transfer	Direct Log-In Access	
Within the Component	X		X	Latent searches, responses, and notifications are exchanged via an electronic connection to and from authorized agencies and the NGI System. Also, the NGI System is interconnected with DoD's and DHS's biometric systems.
DOJ Components	X		X	See above
Federal entities	X		X	See above
State, local, tribal gov't entities	X		X	See above
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments	X			Limited foreign partners have modified access to latent investigative services within the NGI System, which allows for the search and return of only criminal identities. Unidentified latent prints owned by the FBI and having a nexus to terrorism

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.
				are shared with some foreign partners for searches of their biometric systems, and subsequent unidentified latent prints are provided on a recurring basis.
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 latent prints maintained within the NGI System may be used for FBI research and development purposes in accordance with applicable federal law and regulations. When the FBI provides data to NIST it is subject to strict security and use protections pursuant to an interagency agreement between the FBI and NIST. Additional protections are delineated in “Government Furnished Information” letters which the FBI provides to NIST regarding specific research projects and data sets. Any latent prints 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 latent prints 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 latent prints 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 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 latent prints in the NGI System. Quite simply, notice would be impossible because the identity associated with the latent prints is unknown. Also, the FBI has exempted itself from the requirement of 552a(e)(3) for the criminal and national security records maintained in the NGI System. A Privacy

Act notice is provided to individuals when their civil fingerprints are collected for retention in the NGI System. This notice provides specific information regarding the searching of civil prints against latent prints. Therefore, if civil prints are returned as candidates in a latent search, the submitter of the civil prints has received prior notice of this use. The NGI System's SORN provides general notice of the collection and use of latent prints 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 leaving latent prints at a location related to a criminal or national security investigation has no opportunity to refuse the collection of biometrics. It is likely that the individual is not aware that he/she has left latent prints. 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, if applicable.

**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.**

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 pursuant to the Privacy Act. Title 28 CFR 16.30-16.34 establish specific procedures for an individual to obtain a copy of his or her criminal history record from the NGI System for review and correction. Note, however, that the FBI maintains exemptions from access and amendment provisions of the Privacy Act for certain records maintained in the NGI System.

## **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	<p><b>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 23, 2023.</b></p> <p><b>If an ATO has not been completed, but is underway, provide status or expected completion date:</b></p>
---	---

	<b>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:</b> No POAMs related to privacy controls.
	<b>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:</b>
X	<b>Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:</b> The NGI System, including the latent matching service, is continually monitored at the host and network layer. FISMA policy compliance testing occurs monthly.
X	<b>Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:</b> 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	<b>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.</b>
X	<b>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:</b> Pursuant to the CJIS Security Policy, state, local, and tribal 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, including latent prints, is electronically via the CJIS 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 users connect to NGI services via the Law Enforcement Enterprise Portal (LEEP)<sup>5</sup> interface, and authentication of these users occurs at the LEEP interface. Internal (meaning, FBI employee or contractor) NGI general users use a remote laptop connection to a virtual NGI general user workstation via the CJIS WAN virtual private network (VPN) solution using Unclassified

---

<sup>5</sup> 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.

Laptop Management Solution (ULMS). Internal NGI administration personnel use the CJIS WAN VPN solution to connect to a virtual NGI administrator workstation using either NGI-provided laptops or ULMS. Authentication of all internal NGI users using remote access happens both during the VPN connection and at the virtual workstation. Users of the ULMS are also authenticated at the government-provided laptop.

Latent searches received by the NGI System 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. Law enforcement agencies electing to access latent services within the NGI System perform compliance and compatibility testing within the system's nonoperational testing environments to identify and resolve programming limitations prior to implementing full operating capabilities. This nonoperational testing allows compliance problems to be identified and resolved by CJIS and its partner agencies with no harm caused to the accuracy or integrity of the operational system.

In accordance with 28 U.S.C. §534, the FBI does not disclose information from the NGI System, including latent prints 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.

Only authorized criminal justice and national security agencies may search and retain latent prints 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 state and federal agency CJIS Systems Officers (CSOs).

CJIS User Agreements and Outsourcing Standards also define parameters for information sharing. The CJIS Division performs triennial audits of all CJIS system agencies (CSA), the state agencies that are responsible for their states' connections to the NGI System and whose CSOs are responsible for implementing compliance by their states. The state CSOs, in turn, conduct audits of their local agencies on a triennial basis. The state CSO is responsible for implementing and ensuring compliance with the CJIS Security Policy. Likewise, federal agencies with connection to the NGI System have federal CSOs with a similar responsibility at the federal level. 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 state and federal 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. In the specific instance of latent print submissions, the prints must be submitted by vetted and trained personnel of a criminal justice agency.

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.

***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 National Archives and Records Administration (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. Specific to the ULF, as explained earlier in this PIA, latent prints remain in the ULF until the file reaches capacity or are subsequently identified and deleted by the record owners.

## **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, including latent prints, for many decades. Therefore, the searching and retention of latent prints and the release of biometrics in response to those searches within the NGI System does not constitute a new collection type or collection purpose. The latent print submissions generally include no or minimal PII other than the prints themselves; very limited information is provided and collected by the NGI System as the biometric itself is considered unidentified. The information provided and collected is primarily specific to the unique characteristics of the unidentified image and may also include other filters needed for search purposes such as the friction ridge position and pattern type if known or visible. Candidates produced from searches of the latent prints include the associated biometrics needed for comparison purposes, as well as limited biographic information and contact information associated with the event to aid in the investigative process should the comparison result in a positive identification.

As with most biometric searches, there is a risk of misidentification when latent prints are searched within the NGI System and candidates are returned to the user. The FBI recognizes that any biometric capability must be carefully assessed and tested to ensure sufficient reliability and minimum error. The FBI works to continually improve the accuracy of its latent print algorithm and has significantly improved the accuracy with the deployment of the NGI System. In collaboration with NIST, the FBI performs recurring benchmark testing of latent print matching algorithms. Most recently, the FBI initiated an evaluation of latent fingerprint technology with NIST in Fiscal Year 2020. It is expected that this testing will be on-going, and some test results are expected to be returned by the end of 2021. Internally, the FBI monitors the candidates returned in response to search requests and collaborates with the latent user community to refine thresholds and improve latent investigative services within the NGI System. As discussed above, the FBI also provides non-operational testing environments within the NGI System so that submitters of latent prints may perform testing with no impact to the operational environment. The FBI continuously tests and evaluates latent services within the NGI System to negate impacts to performance or accuracy prior to deployment of subsequent system modifications and enhancements.

Only authorized law enforcement and national security agencies have the ability to search and retain latent prints within the NGI System for investigative lead purposes. The FBI has promulgated policies and procedures to emphasize that candidates returned from the NGI System are considered investigative leads. The returned candidates must be evaluated by latent print examiners within the receiving agency to determine if any candidate results in a positive identification. Latent print examiners, whether employed within the FBI's Laboratory Division or other federal or state laboratories, must be certified according to national scientific standards for latent print examination. If retained within the ULF, record owners have the ability to delete those subsequently identified or when the crime is no longer actionable or exceeds statute limitations. As discussed in this PIA, the CJIS Division establishes the use policy and technical requirements for the submission of latent prints to the NGI System; however, it is also the responsibility of the participating agencies to develop appropriate use policies in accordance with the applicable laws and policies of their relevant governmental jurisdictions. All appropriate use policies must protect the Constitutional rights of all persons.

Because latent print services reside within the NGI System, all latent users must comply with pre-existing NGI requirements and policy. In particular, the agencies 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 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. Although latent prints are unidentified in nature, the same system security, audit oversight, and policy requirements apply to these unknown persons.

The privacy risk of maintaining erroneous or unauthorized latent prints is further mitigated by the actions taken by the FBI, in compliance with law and policy, to ensure the accuracy of the information within the NGI System. 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 system and to conduct ongoing reviews of the information residing in the system. Additionally, the maintenance and dissemination of information must comply with the provisions of any applicable law, regulation, or policy, including the Privacy Act of 1974. Among other requirements, the Privacy Act obligates the FBI to make reasonable efforts to ensure that records it disseminates to non-federal agencies is accurate, complete, timely, and relevant. 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.