Federal Bureau of Investigation

Privacy Impact Assessment
for the
Next Generation Identification
Interstate Photo System

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:

(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 Federal Bureau of Investigation's (FBI's) PIA for the Next Generation Identification (NGI) Interstate Photo System (IPS) issued in October 2019. The NGI System serves as the FBI's biometric identity and criminal history records system[1] and maintains the fingerprints and associated identity information of individuals submitted to the FBI for authorized criminal justice, national security, and civil purposes. The NGI IPS contains the photos collected by federal, state, local, tribal, and territorial agencies submitted with tenprint fingerprints. The NGI IPS offers a facial recognition (FR) search capability to law enforcement (LE) users of the criminal photos (i.e., "mugshots") maintained in the system. This PIA describes the current use of the NGI IPS since its development in 2015.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

The NGI IPS currently contains face photos as well as photos of scars, marks, and tattoos. Photos submitted to the NGI IPS are received voluntarily with tenprint fingerprint transactions from authorized federal, state, local, tribal, and territorial agencies. The NGI IPS photos are associated to the FBI Universal Control Number (UCN). A UCN is a unique identity number in the NGI System, which links the photos with tenprint fingerprints and related biographic and biometric information in the NGI System. Submitted images are housed together in a common repository, logically separated into criminal, civil[2], and national security[3] identity groups. This logical separation provides system flexibility to maintain handling and dissemination of information. The automated NGI IPS FR algorithm is applied to each of the submitted images to determine if the image is of sufficient quality

[1] *See* NGI System of Records Notice (SORN), 81 Fed. Reg. 27,284 (May 5, 2016); 82 Fed. Reg. 24151, 156 (May 25, 2017); 84 Fed. Reg. 54,182 (Oct. 9, 2019).
[2] Civil fingerprints are submitted to the FBI for criminal background checks for non-criminal justice purposes, such as employment, licensing, government benefits, and security clearances. Although uncommon, a civil photo may be included with the fingerprint submission. Civil photos are not available for searching or dissemination to law enforcement agencies except when an individual also has a record in the criminal identity group. In this instance, all biometrics, including photos, become associated with the criminal identity group and are available for searching and dissemination.
[3] Although national security photos are retained in the NGI System, their dissemination is strictly controlled by the FBI CJIS Division and the owners of the records. In general, national security photos are not disseminated to state and local law enforcement agencies unless the owner of the national security record coordinates with the LE submitter of the probe photo in the event of a potential investigative lead. Otherwise, the LE submitter will have no knowledge of the record.

for search; and, if so, the algorithm creates a face template. Although a template may be created for images in any of the three identity groups, FR searches (FRSs) of the NGI IPS are conducted only against the criminal photos and are not conducted against face images associated with a civil-only identity in the NGI System.

The NGI IPS also provides an investigative FRS capability limited to law enforcement agencies (LEAs). LEAs are permitted to search photos obtained related to criminal investigations, known as "probe" photos, against the photos maintained in the NGI IPS. Authorized users conducting FRSs against the NGI IPS must comply with FBI policy regarding use of the system. FBI policy defines probe photos as facial photos lawfully obtained pursuant to an authorized criminal investigation. FBI policy prohibits the submission of photos of individuals exercising rights guaranteed by the First Amendment (e.g., lawful assembly) unless pertinent to and within the scope of an authorized LE activity. The policy also prohibits submission of photos collected as a result of a search in violation of the Fourth Amendment. After the FRS is performed, the probe photo is not retained in the NGI IPS.

The automated FR algorithm in the NGI IPS compares the probe photo against the photos in the NGI IPS to locate potential candidate photos. The algorithm uses pattern-matching approaches developed within the field of computer vision to identify people in photos from their facial appearance. Patterns are groups of numbers that summarize the image of a face, or a part of a face, in a way that is supposed to preserve identity information. The distance between two patterns[4] should be low for two images of the same person and high for images of different people. The software that computes the pattern may be written to take advantage of the anatomy of the face but also uses inputs such as lighting, facial surface changes like facial hair or cosmetics, and facial modifications due to changed expressions, such as closed eyes, wrinkled brow, etc. Although anatomical features are very important, the performance of the algorithm ultimately depends upon the patterns which the algorithm developer found to be most useful for matching. The algorithm uses these features to create a template from the face, which is then compared against other face templates.

Since the NGI IPS is designed to provide investigatory leads, rather than an identification, a gallery of potential candidate photos will always be returned to the LEA. The candidate gallery returned to the LEA will generally consist of an array of two or more photos associated to a criminal identity. Specifically, a single photo will never be returned, but a gallery of two to fifty photos, with the LEA choosing the size of the gallery. If no choice is made, a default of twenty photos is returned. In addition, the UCN, subject's name, biometric set identifier (a unique number assigned to each biometric image), and the match score are returned with each candidate photo. The recipient LEA may choose what data points are viewable by its biometric examiners.

Candidate photos returned to the LEA are provided as investigative leads only and not as positive identification. Although FR technology has become increasingly accurate, authorized users of the NGI IPS are prohibited from relying solely on the candidate photos to conduct LE action. The candidate photos must be considered as investigative leads only; identity must be established in conjunction with other relevant identifying information and evidence related to the criminal

[4] The patterns used in the NGI IPS algorithm may not correlate to obvious biological anatomical features such as the eyes, nose, or mouth.

investigation. A caveat is added to all candidate photos returned from the NGI IPS which states, *"This response is an INVESTIGATIVE LEAD ONLY. It is NOT positive identification of the subject. If you are not the intended recipient, you are hereby notified of your responsibility to immediately email the sender and, following notification to sender, to delete this email and all of its attachments."*

FBI policy requires that LEA users complete FR training in compliance with national scientific guidelines prior to conducting FRSs of the NGI IPS. States and agencies with the capability to conduct FRSs of the NGI IPS have been notified of the training requirement, which may be met either through vendor or FBI provided training. Training must meet the Facial Identification Scientific Working Group (FISWG) guidelines.[5]

With this training, the LEA user learns how to conduct an effective manual review of the candidate photos to determine whether the gallery contains a likely candidate to the probe photo. If the LEA user determines a likely candidate, the LEA user will then proceed with additional evaluation and investigation to determine if the probe photo and the candidate photo are, in fact, the same subject.

To conduct FRSs of the NGI IPS, the LEA's information system must be programmed to submit and receive FR transactions electronically and must successfully complete testing with the FBI. Currently, there are two federal agencies and 17 state jurisdictions with the technical capability to conduct FRSs. The probe photos received for LE purposes from all federal and state LEAs are processed by the FBI under rules detailed in the *NGI IPS Policy and Reference Guide*[6] with candidate photos returned as investigative leads.

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; 34 U.S.C. §10211; 44 U.S.C. §3301; 6 U.S.C. § 211(g)(4)(C); Uniting and Strengthening America by Providing Appropriate Tool Required to Intercept and Obstruct Terrorist (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001)
Executive Order	Executive Orders 8781, 8914, and 13764
Federal regulation	28 C.F.R. 0.85, 20.31, 20.33
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	

[5] Refer to www.FISWG.org for training guidelines.
[6] The *NGI IPS Policy and Reference Guide* describes the policy and technical requirements for authorized use of the NGI IPS, as well as the best practices for NGI IPS users.

Section 3: Information in the Information Technology

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

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name			
Date of birth or age			
Place of birth			
Sex			
Race, ethnicity or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
E-mail addresses (personal, work, etc.) Please describe in Comments			
Phone numbers (personal, work, etc.) Please describe in Comments			
Medical records number			
Medical notes or other medical or health information			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
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			
Juvenile criminal records information			
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:			
- **Photos or photographic identifiers**	X	A, B, C, 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
- **Video containing biometric data**			
- **Fingerprints**[7]			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**	X	A, B, C, D	
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**	X	A, B, C, D	The FBI UCN associated with the photo, excluding civil-only identities, will also be disseminated. This is used to link the photo with biometric and other biographic data in NGI. However, NGI IPS does not itself contain identifiers beyond what is checked in the instant chart.
System admin/audit data:		A, B, C, D	Non-federal users would be state, local, and tribal LE users (applicable to all in this section).

[7] While photographs are submitted with tenprints, they are not maintained together.

(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
- **User ID**	X	A	Access to NGI IPS is limited to internal FBI users from CJIS. Any other foreign or domestic law enforcement agency must submit an FRS request using their agencies Originating Agency Identifier (ORI)/Controlling Agency Identifier (CRI) combination and their own system. As such, NGI/IPS does not contain usernames and passwords for these users. Federal and state CSOs must apply to the FBI CJIS Division for the assignment of ORIs/CRIs and FBI CJIS Division staff evaluates these requests to ensure the agency or entity meets the criteria for the specific type of ORI/CRI requested. The ORI/CRI provides the correct level of access to CJIS Systems (i.e., NGI System) and the ORI/CRI controls the dissemination of information. This access is strictly controlled and audited by the FBI CJIS Division. The FBI CJIS Division maintains an index of ORIs/CRIs and logs each dissemination of identification records to the applicable ORI/CRI.
- **User passwords/codes**		A	Access to NGI IPS is limited to internal FBI users from CJIS. A law enforcement agency must submit an FRS request using their agencies ORI/CRI combination and their own system. As such, NGI/IPS does not contain usernames and passwords for these users.
- **IP address**	X	A, B, C, D	
- **Date/time of access**	X	A, B, C, D	
- **Queries run**	X	A, B, C, D	
- **Content of files accessed/reviewed**	X	A, B, C	If required by the System Administrator (SA).
- **Contents of files**	X	A, B, C	If required by the SA.
Other (please list the type of info and describe as completely as possible):			

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

Directly from the individual to whom the information pertains:					
In person	X	Hard copy: mail/fax		Online	
Phone		Email			
Other (specify): Only photos obtained by DOJ components (such as a photo taken pursuant to a federal arrest) will be taken directly from the individual. Most photos in the NGI IPS are submitted by other government partners.					

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

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

Section 4: Information Sharing

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

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component			X	Authorized FBI users may search probe photos against the photos in the NGI IPS. Candidate photos are the only results returned from these queries. See Section 2 for more information.
DOJ Components			X	Authorized LE users within DOJ may search probe photos against the photos in the NGI IPS. Candidate photos are the only results returned from these queries. See Section 2 for more information.
Federal entities			X	Authorized LE users from federal agencies may search probe photos against the photos in the NGI IPS. Candidate photos are the only results returned from these queries. See Section 2 for more information.
State, local, tribal gov't entities			X	Authorized LE users from local, state, and tribal entities may search probe photos against the photos in the NGI IPS. Candidate photos are the only results returned from these queries. See Section 2 for more information.
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 photos maintained in the NGI IPS may be used for FBI research and development purposes in accordance with applicable federal law and regulations. In particular, the FBI works with the National Institute of Standards and Technology (NIST)[8] to ensure that its FR and other biometric technology is of the highest standards. When the FBI provides data to NIST, it is subject to strict security and use protections. The NGI IPS photos used for research and development are sent without additional personally identifiable information (PII), such as the UCN, fingerprints, or biographic data. The data is encrypted in accordance with Federal Information Processing Standards (FIPS) 140-2 requirements prior to release. The data is stored in laboratories which have received an authority to operate (ATO) in accordance with FBI security policy and the Federal Information Security Modernization Act of 2022. In addition, only those with documented authorization and a true need-to-know are granted access to the photos. No NGI IPS data is 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 photos in the criminal or national security identity groups of the NGI IPS. Also, the FBI has exempted itself[9] from the requirement of 552a(e)(3) for the criminal and national security records maintained in the NGI System. However, the photos are collected in conjunction with tenprint fingerprints, which means the subject should be aware of the collection. Only individuals in the NGI IPS Civil Identity Group of the NGI IPS will receive a Privacy Act notice concerning the collection of their fingerprints, photos, and other personally identifiable information when applying for employment and licensing. The FBI maintains exemptions from the requirement of 552 a(e)3 for records outside of this identity group. The NGI SORN provides general notice of the collection and use of the photos. This PIA also provides general notice, as does the previously published PIA regarding the NGI IPS. There is no notice for individuals captured in probe photos, as those individuals are unknown to the submitter and are the subject of a law enforcement investigation.

[8] NIST is one of the nation's oldest physical science laboratories. Its core competencies include measurement science, rigorous traceability, and development and use of standards. It is part of the Department of Commerce.
[9] *NGI System of Records Notice (SORN)*, Federal Register; Next Generation Identification System, 81 Fed. Reg 27, 284 (May 5, 2016), 82 Fed. Reg. 24151 (May 25, 2017); 84 Fed. Reg. 54,182 (Oct. 9, 2019).

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.

A person under arrest or the subject of an investigation may have no opportunity or right to refuse the collection of biometrics. Nevertheless, any criminal or national security uses of the information must comply with the provisions of applicable law, including 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.

Title 28 Code of Federal Regulations (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	**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 LE 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, including the NGI IPS, 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.
	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, LE users and appropriate FBI/contract staff 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 main method for the transmission of biometric submissions is electronically, via the CJIS Wide Area Network (WAN), a telecommunications infrastructure that connects authorized agencies to the FBI CJIS Division host computer systems. The role of the CJIS WAN is to provide a secure transport

mechanism for the FBI CJIS Division criminal history record information and biometric-related information. The WAN provides direct and indirect electronic access to FBI identification services and data for numerous federal, state, local, tribal, and territorial LEAs in all fifty states. Agencies transmit and, in turn, the FBI CJIS Division responds via the CJIS WAN. Transmission hardware for the CJIS WAN is configured by FBI personnel, the transmission data to and from the FBI CJIS Division is encrypted, and firewalls are mandated and in place.

Internal (meaning, FBI employee or contractor) NGI System general users use a remote laptop connection to a virtual NGI System general user workstation via the CJIS WAN virtual private network (VPN) solution using Unclassified Laptop Management Solution (ULMS). Internal NGI System administration personnel use the CJIS WAN VPN solution to connect to a virtual NGI administrator workstation using either NGI System-provided laptops or ULMS. Authentication of all internal NGI System 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.

Electronically, the biometrics will be supported through the Electronic Biometric Transmission Specification (EBTS), which currently supports fingerprint, palm print, latent print submissions, and face and scar, mark, and tattoo photos. The EBTS provides proper methods for external users to communicate with the FBI CJIS Systems for the transmission of biographic and biometric information for purposes of criminal or civil identification. The FBI developed the EBTS standard for electronically encoding and transmitting biometric image, identification, and arrest data that extends the America National Standards Institute/NIST – 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 the guidelines for the exchange of information between various federal, state, local, tribal, territorial, and international biometric systems, the FBI's EBTS defines requirements to which agencies must adhere when electronically communicating with the NGI System.

Additional privacy protections are provided by 28 U.S.C. §534, which states that the dissemination of information under its authority is subject to cancellation if shared information is disclosed outside the 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*.[10]

Only authorized users can gain access to conduct an FRS within the NGI IPS. System access lists are updated as personnel change job positions or leave FBI service. The NGI IPS provides access and authentication to system level information based upon the authorized General User (external user of the system) and Privileged User (system administrator) access. General Users submit FRSs to the NGI IPS. Privileged Users are provided with the capabilities to view submission data for purposes linked to NGI System administration. This includes the ability to view probe photos for the purpose of

[10] The CJIS Security Policy can be found here: https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center

troubleshooting submissions. All General User and Privileged User actions are logged in the system audit logs with full traceability to users performing actions. All system audit logs are retained in accordance with FBI retention policies and guidelines. General Users of the NGI IPS 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 FBI CJIS Division performs triennial audits of all CJIS system agencies (CSA), the state agencies that are responsible for their states' connections to the NGI IPS 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 a connection to the NGI IPS have federal CSOs with a similar responsibility at the federal level. The FBI CJIS Division provides training assistance and up to date materials to each CSO and periodically issues information 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 FBI CJIS Division and CSA audits confirm that only authorized agency personnel are accessing the NGI IPS for authorized purposes.

The audits assess and evaluate users' compliance with the FBI 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 Originating Agency Identifier (ORI). Federal and state CSOs must apply to the FBI CJIS Division for the assignment of ORIs and FBI CJIS Division staff evaluates these requests to ensure the agency or entity meets the criteria for the specific type of ORI requested. The ORI provides the correct level of access to CJIS Systems, and the ORI controls the dissemination of information. 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 FBI CJIS Division. The FBI 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 NGI System data, including the photos in the NGI IPS, are retained in accordance with the applicable retention schedule approved by the National Archives and Records Administration. NARA has approved the destruction of fingerprints and associated information, including other biometrics, when criminal and civil subjects attain 110 years of age. NARA has determined automated FBI criminal history information and NGI System transaction logs are to be permanently retained. Biometrics such as photos 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. The FBI does not retain any of the probe photos that are searched against the NGI IPS.

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 photos in the NGI IPS including those photos in the UPF do not constitute a new collection type or collection purpose. Instead, the NGI IPS provides the significant enhancement of FR technology for these photos.

The retention of photos and the searching and dissemination of these photos based on FR technology presents a risk of erroneous identification. FR searching of the photos, excluding photos associated to a civil-only identity, entails the risk that the technology may not be sufficiently reliable to accurately locate other photos of the same identity, resulting in an unacceptable percentage of misidentifications. The FBI recognizes that any biometric capability must be carefully assessed and tested to ensure sufficient reliability and minimum error.

The FBI has conducted tests, which verified the NGI IPS is sufficiently accurate for all allowable candidate list sizes according to system requirements. The FBI has also evaluated detection rates for all allowable candidate list sizes ranging from two to fifty. Detection rates were verified to meet system requirements for each list size. Traditionally, NIST benchmark testing was performed approximately every three to four years. However, due to the speed at which technology advances, traditional methods no longer permit the level of technology awareness the FBI desires. Ongoing FR testing performed by NIST enables the FBI to test its NGI IPS FR technology annually, as well as permit other vendors to submit FR algorithms to NIST at least once a year. NIST testing focuses primarily on algorithm accuracy across the following categories: overall accuracy (all categories combined), accuracy across demographics (i.e., sex, race, age, twins, etc.), and accuracy based on image properties (i.e., mugshot photos, unconstrained photos, poor quality photos, etc.). The FBI's latest algorithm, installed on 01/21/2024, achieves accuracy rates of over 99 percent in current NIST testing for all candidate list sizes.

Internally, the FBI monitors the candidate photos returned to requesters in response to FRSs and works with those requesters in refining thresholds to improve the success of investigative FRSs performed in the NGI IPS. In addition, the FBI performs regression and baseline tests on the FBI test environments, which have been established with data and environments that are scaled representatives of the NGI IPS operational environment. The FBI continuously tests and evaluates the NGI IPS with each system enhancement, new algorithm installation, or other changes to ensure that accuracy and system performance are not negatively affected. The FBI CJIS Division designed an FR operational evaluation tool that performs an annual FR analysis of the NGI IPS operational environment. This evaluation tool ensures optimal performance, system integrity, data consistency as the NGI System changes over time due to architectural design (e.g., infrastructure or code); new or removed gallery enrollments; and/or vendor algorithm upgrade/enhancements. For the past several years, the FBI CJIS Division has used this operational evaluation tool.

Although FR technology continues to improve, the FBI only permits the NGI IPS to be used as an investigative lead. The FBI has promulgated policies and procedures to emphasize that photos returned from the NGI IPS are not to be considered "positive" identifications, and searches of the NGI IPS will merely result in a ranked listing of candidate photos from the NGI IPS, the search result will include a specific caveat advising that the photos are to be used for investigative lead purposes only

and that further investigation is required to determine the subject's identity.

Photos submitted to the NGI IPS for retention by authorized users must meet the requirements as described in Section 2. In addition, it is the responsibility of the participating LEAs to develop appropriate use policies for NGI IPS FRS, 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. The LEA users must also ensure compliance with the *CJIS Security Policy*, CJIS User Agreement, and the *NGI IPS Policy and Reference Guide*. The *NGI IPS Policy and Reference Guide* expressly prohibits collection of probe photos in violation of an individual's First and/or Fourth Amendment rights.

The FBI made several decisions to protect privacy and civil liberties when it developed the FR capability within the NGI IPS. The FBI does not permit the searching or dissemination of civil photos in its repository. These photos were submitted for authorized noncriminal justice purposes, such as employment, licensing, and security clearances. By limiting the searchable photo repository, the FBI ensured that only those photos collected pursuant to a lawful LE purpose and positively associated with tenprint fingerprints would be available for searching. Further, to maintain the integrity of the NGI IPS, the FBI does not retain any of the probe photos that are searched against the NGI IPS. Although the probe photos must be obtained in furtherance of a LE investigation and must be collected in compliance with law and policy, such photos are not retained in the NGI IPS.

The FBI also instituted additional privacy and civil liberties protections while developing the UPF. Since the FBI would be maintaining photos of unknown persons in its repository, it required that the alleged crime must be a felony against a person, and it required frequent validation and review of the submitted photos. The FBI placed these safeguards to ensure that the file is not misused and to ensure that photos are removed as soon as there is no longer an investigative interest in that person. In addition, the same system security, audit oversight, and policy requirements of the NGI IPS apply to these photos of unknown persons.

The increased retention of photos presents a correspondingly increased risk that the information may potentially be subject to loss or unauthorized use. The strong security features and robust audit processes already present in the NGI System mitigate this risk. The FBI CJIS Division's Audit Unit continues to conduct audits of federal, state, local, tribal, and territorial agencies enrolling and/or searching photos in the NGI IPS. The NGI IPS audits continue to be conducted in conjunction with pre-established National Identity Services triennial audits. In addition, the system stores information regarding the dissemination of photos and related data for audit logs. Dissemination of information is linked to the authorized NGI IPS user or the agency that requested the photo. This information is incorporated into the audit process and provides an enhanced capability for ensuring the information is being appropriately used and disseminated. Agencies requesting and receiving photos will be subject to training and audit requirements by the applicable state or federal agency and periodic FBI audit.

The increased retention and searching of photos in the NGI IPS present a privacy risk that the photos will be searched and used for purposes unknown to the individual who provided the photo. It also creates a risk that the photos will be disseminated for unauthorized purpose or to unauthorized recipients. Another privacy risk could be the improper access to the data or misuse of information in the NGI System, such as unauthorized electronic searching of the photos in the NGI IPS. These risks

are mitigated through the NGI System's strict system security requirements and user rules regarding access and dissemination, as well as the periodic audits conducted by the FBI to ensure that system searches are relevant and necessary to the person's official duties. The system stores information regarding the dissemination of photos and related information in audit logs but does not retain the actual probe photos. Dissemination of information is linked to the authorized user and the agency that requested the information. The FBI CJIS Division's Audit Unit regularly visits agencies that are authorized to collect and submit photos. Allegations of misuse of FBI CJIS Systems, including the NGI System, are generally referred to the appropriate CSO of the jurisdiction where the misuse occurred, and the FBI responds to all such allegations.

The FBI has a substantial interest in ensuring the accuracy of the information in the system, and in taking action to correct any erroneous information of which it may become aware. The maintenance and dissemination of information must comply with the provisions of any applicable law, regulation, or policy, including the Privacy Act. Among other requirements, the Privacy Act obligates the FBI to make reasonable efforts to ensure the information that it disseminates to non-federal agencies is accurate, complete, timely, and relevant.