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: [10/29/19

(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 Federal Bureau of Investigation's (FBI's) PIA for the Next Generation Identification (NGI) Interstate Photo System (IPS) issued in September 2015. 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 both criminal and civil photos submitted with ten-print fingerprints and offers a facial recognition search capability to law enforcement users. This PIA describes the current use of the NGI-IPS since its development in 2015, as well as planned new functionality, including the implementation of the Unsolved Photo File (UPF) and the use of the facial recognition search capability by components of the Department of Homeland Security (DHS).

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 over 93 million civil photos, criminal photos, and scars, marks and tattoo images. Of this number, over 38 million criminal photos are available for facial recognition searching by law enforcement agencies. The number of photos enrolled in the NGI-IPS and the number of facial recognition searches performed against the NGI-IPS is expected to grow based on the use of facial recognition by federal, local, state, and tribal law enforcement agencies. The civil and criminal photos are separated into respective Identity Groups.

Criminal Identity Group:

Authorized law enforcement agencies may submit and enroll photos (i.e., mugshots) taken pursuant to arrest and associated with criminal ten-print fingerprints for retention in the Criminal Identity Group of the NGI-IPS. The submission of these photos to the NGI-IPS is voluntary by local, state, tribal, and federal law enforcement agencies. Selected foreign and international law enforcement agencies may also contribute criminal photos for retention in the NGI-IPS, but may not search the NGI-IPS. The mugshots must meet technical specifications in order to be enrolled in the NGI-IPS and the FBI has provided training to law enforcement agencies regarding best practices for the taking of mugshots.

[1] *See* NGI System of Records Notice, 81 Fed. Reg. 29,284 (May 5, 2016); 84 Fed. Reg.54, 182 (October 9, 2019).

The NGI-IPS also provides an investigative facial recognition search capability limited to law enforcement agencies. Law enforcement agencies are permitted to search criminal investigatory photos, known as "probe" photos, against the criminal mugshots maintained in the NGI-IPS. Authorized users conducting facial recognition searches 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 law enforcement activity. The policy also prohibits submission of photos collected as a result of a search in violation of the Fourth Amendment. After the facial recognition search is performed, the probe photo is not retained in the NGI-IPS. This ensures that the Criminal Identity Group of the NGI-IPS remains a repository of mugshots collected pursuant to arrest.

The automated facial recognition algorithm in the NGI-IPS compares the probe photo against the mugshots in the Criminal Identity Group in order to find candidate photos. The algorithm uses pattern-matching approaches developed within the field of computer vision to identify people in photographs 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 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. The patterns used in the NGI-IPS algorithm may not correlate to obvious biological anatomical features such as the eyes, nose or mouth. 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.

Because the NGI-IPS is designed to provide investigatory leads, rather than an identification, a gallery of candidate photos will always be returned to the law enforcement agency. A gallery of two to fifty photos will be returned, with the law enforcement agency choosing the size of the gallery. If no choice is made, a default of twenty photos is returned.

Candidate photos returned to the law enforcement agency are provided as investigative leads only and are not positive identification. Although facial recognition technology has become increasingly accurate, authorized users of the NGI-IPS are prohibited from relying solely on the candidate photos to conduct law enforcement action. The candidate photos must be considered as investigative leads only, in conjunction with other relevant information and evidence related to the criminal investigation. A caveat will be added to all candidate photos returned from the NGI-IPS which states, "*The information returned in response to this request is provided as an INVESTIGATIVE LEAD ONLY and is NOT to be considered a positive identification.*"

FBI policy requires that law enforcement agency users complete facial recognition training in compliance with national scientific guidelines prior to conducting facial recognition searches of the NGI-IPS. States with the capability to conduct facial recognition searches 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 guidelines.[2]

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

In order to conduct a facial recognition search of the NGI-IPS, the law enforcement agency's information system must be programmed to submit and receive facial recognition transactions electronically and must successfully complete testing with the FBI. At this time, the following jurisdictions have the technical capability to conduct facial recognition searches: Michigan, Arkansas, Texas, Maine, New Mexico, Delaware, District of Columbia, South Carolina, West Virginia, Arizona, Louisiana, Hawaii, Kentucky, Missouri, Iowa, and Colorado. The only federal entity currently performing facial recognition searches of the NGI-IPS is the FBI's FACE Services Unit.

All federal law enforcement agencies, including law enforcement components of the Department of Homeland Security (DHS), are authorized to enroll and search photos in the NGI-IPS for legally authorized purposes. The FBI expects that the National Targeting Center (NTC), within the U.S. Customs and Border Protection (CBP) agency, will access the NGI-IPS for the purpose of conducting individualized facial recognition searches for law enforcement purposes. The NTC is responsible for a potentially wide array of duties, such as collecting and analyzing traveler information in advance of arrival in the United States to identify and address security risks; coordinating the examination of entry and exit of travelers; identifying, reviewing, and targeting travelers for examination, and other duties and powers prescribed by the Executive Assistant Commissioner. *See* 6 U.S.C. Section 211(g)(4)(C).

When using the NGI-IPS, however, the NTC will be limited to using its screening rules to identify the small percentage of travelers whose photos will be sent on an individualized basis to the NGI-IPS for a facial recognition search when there is a law enforcement purpose; and these photos will be processed by the FBI under rules detailed in the FBI's NGI-IPS Policy and Implementation Guide, including limitations for law enforcement purposes. The DHS NTC screening rules are used to determine on an individualized basis which travelers are reasonably suspected to pose a risk to border security or public safety, who may be a terrorist or suspected terrorist, who may be inadmissible to the U.S., or who may otherwise be engaged in activity in violation of U.S. criminal law. As with all users, the candidate photos returned to the NTC are for lead purposes only, cannot be used for positive identification, and the NTC must perform additional research to resolve the identities of the subjects before taking any action.

Civil Identity Group:

Civil fingerprints are submitted to the FBI for criminal background checks for non-criminal justice purposes, such as employment, licensing, and security clearances. These fingerprints are submitted pursuant to federal statutes, executive orders, state statutes in accordance with Public Law 92-544, and other legal authorities. In some instances, the civil fingerprint contributors may choose to submit the

[2] Refer to www.FISWG.org for training guidelines.

photos of applicants, employees, licensees, and those in positions of public trust. These civil photos (i.e., not associated with any criminal history) are maintained in the Civil Identity Group of the NGI-IPS and are not searched by or against photos maintained in the Criminal Identity Group. These civil photos contained in the Civil Identity Group are not disseminated to law enforcement agencies or shared with any agency other than the original contributor of the photo. Likewise, the non-criminal justice agencies and entities that submit civil photos are not permitted to perform searches of the criminal photos in the NGI-IPS.

The only exception to the non-searching and non-dissemination of the civil photos occurs when an individual has a record in both the Civil Identity Group and the Criminal Identity Group (e.g. fingerprints have been collected for employment and, separately, for arrest purposes). In this instance, all collected biometrics, including photos, become associated with the Criminal Identity Group. The individual's photo, although originally submitted for civil purposes, becomes a photo that is searched and disseminated according to the Criminal Identity Group rules. This enables NGI to function as a "one-identity" system to ensure that the criminal identity records contain the most complete and accurate information. In circumstances where the individual's identity within the Criminal Identity Group is removed (e.g. expunged), the civil photo will be electronically returned to the Civil Identity Group, and will no longer be searched or disseminated.

Unsolved Photo File:

The FBI plans to implement the Unsolved Photo File (UPF) as a sub-file of the NGI-IPS. The UPF will be populated with law enforcement photos of unknown subjects. As with the Criminal Identity Group, only authorized law enforcement agencies may enroll and search photos in the UPF. The criteria for enrollment is as follows:

(1) The photo must be obtained pursuant to a reasonable suspicion of criminal activity in the course of an active law enforcement investigation;
(2) The criminal activity must be a felony crime against a person in the relevant jurisdiction;
(3) The photo enrollment must include the appropriate National Crime Information Center (NCIC) code/crime type; and,
(4) The location and identity of the subject must be unknown.

Prior to enrollment in the UPF, the law enforcement agency user must submit the photo for a search against the mugshots in the NGI-IPS. If that search does not produce a likely candidate from the gallery and the subject remains unknown, the contributor may choose to enroll the photo in the UPF, if it meets enrollment criteria. When new photos are submitted for inclusion into the UPF, they will be searched against all of the current mugshots in the NGI-IPS. Likewise, all mugshots will search against the UPF when submitted for enrollment in the Criminal Identity Group of the NGI-IPS. The Criminal Identity Group will remain a repository for mugshots taken pursuant to arrest, and will not retain any photos enrolled in the UPF. Photos maintained in the Civil Identity Group will not be searched by or against the UPF.

If a law enforcement agency user wants to search a probe photo against the UPF, he or she must affirmatively request that the search include the UPF in addition to the search of the mugshots in the NGI-IPS. Upon searching the UPF, if a photo in the UPF scores above a specific threshold, an Unsolved Biometric Message (UBM) will be generated to the owner of the UPF photo and the

candidate photo that scored above the threshold will be sent to the owner of the UPF photo. Only photos associated with a criminal identity will generate a UBM and be sent to the owner of the UPF photo. In the case of a photo enrollment, the photo would search the UPF but no UBM is sent to the submitter of the photo. A direct search of the NGI-IPS is an investigative search and does not search against the UPF so no UBM would be generated.

All photos enrolled in the UPF will be required to be validated by the contributors within six months of enrollment, to ensure that reasonable suspicion of the subject's commission of a felony crime against a person remains. Also, if a photo remains in the UPF for one year, the contributor will be required to validate the photo annually or delete it from the system.

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
X	Statute	28 U.S.C. §§ 533, 534; 42 U.S.C. § 3771; 44 U.S.C. § 3301; 6 U.S.C. § 211(g)(4)(C); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorist (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).
X	Executive Order	Executive Orders 8781, 8914, and 10450.
X	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)	

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[3]			
Date of birth (DOB) or age			
Place of birth			
Gender			
Race, ethnicity or citizenship			
Religion			
Social Security Number (SSN) (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			
Personal e-mail address			
Personal phone number			
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			

[3] The NGI-IPS contains only photos with associated Universal Control Numbers (UCN). A UCN is a unique identity number in NGI, which links the photo with biographic and other biometric information in NGI.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, D	
- **Video containing biometric data**			
- **Fingerprints**[4]			
- **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)**			
System admin/audit data:		A, B	Non-federal users would be state, local and tribal law enforcement users (applicable to all in this section).
- **User ID**	X	A, B	
- **User passwords/codes**	X	A, B	
- **IP address**	X	A, B	
- **Date/time of access**	X	A, B	
- **Queries run**	X	A, B	
- **Content of files accessed/reviewed**	X	A, B	If required by the System Administrators

[4] While fingerprints are submitted to the FBI with photos, they are not collected or maintained in the NGI-IPS system.

(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
- **Contents of files**	X	A, B	If required by the System Administrators
Other (please list the type of info and describe as completely as possible):	x	A, B	The FBI UCN associated with the photo in the Criminal Identity Group will also be disseminated.

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 mugshot taken pursuant to a federal arrest) will be taken directly from the individual. The vast majority of photos in the NGI-IPS are submitted by other government partners.					

Government sources:					
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): Canada is permitted to enroll photos in the Criminal Identity Group of the NGI-IPS but is not permitted to perform facial recognition searches.					

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 Criminal Identity Group and the UPF. Candidate photos are the only results returned from these queries. See Section 2 for more information.
DOJ Components			X	Authorized law enforcement users within DOJ may search probe photos against the Criminal Identity Group and the UPF. Candidate photos are the only results returned from these queries. See Section 2 for more information.
Federal entities			X	Authorized law enforcement users from federal agencies may search probe photos against the Criminal Identity Group and the UPF. Candidate photos are the only results returned from these queries. See Section 2 for more information.
State, local, tribal gov't entities			X	Authorized law enforcement users from local, state, and tribal entities may search probe photos against the Criminal Identity Group and the UPF. Candidate photos are the only results returned from these queries. See Section 2 for more information.
Public				

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.**
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) to ensure that its facial recognition and other biometric technology is of the highest standard. 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 names, the UCN, or full date of birth; however, some non-unique biographic information, such as year of birth and sex, as well as other biometrics may accompany the photo. Non-unique biographic information and other biometrics (limited to fingerprint, palm, iris) accompany the photo only when required by the given research activity. 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. 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 mugshots in the Criminal Identity Group of the NGI-IPS. The FBI maintains exemptions from the requirement of 552a(e)(3) for the criminal records maintained in NGI. However, the mugshot photos are collected in conjunction with ten-print fingerprints upon arrest and the subject should be aware of the collection. The NGI System of Records Notice (SORN) provides general notice of the collection

and use of the mugshots 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 PIA regarding the NGI-IPS, which may be found at https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments. Although the photos in the Civil Identity Group of the NGI-IPS are not searched or shared, civil applicants receive an FBI Privacy Act notice upon collection of their fingerprints and other PII when applying for employment or licensing.

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. For civil applicants, the choice to apply for employment or licensing is voluntary and they may decline to provide the requested information.

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 NGI.

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).

	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): October 24, 2018
	If an ATO has not been completed, but is underway, provide status **or expected completion date:**
X	**Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs)**

	for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The NGI System is under continuous monitoring for performance and security using system and enterprise monitoring approaches.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** The NGI System logs are sent real time to the CJIS Security Operations Center (SOC) and Network Operations Center (NOC) for constant monitoring and are forwarded to FBI Enterprise Security Operations Center (ESOC) monitoring service. This includes monitoring of frequent network activities to prevent against intrusion, illegal or improper use, and security vulnerabilities. Additionally, the System Security Administrator reviews log files in accordance with FBI policies directed by NIST 800-53. Reviews are held monthly at a minimum, or more frequently as needed.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** Anyone accessing the NGI System is required to take mandatory annual security training prior to access. Additionally, privileged users take annual training focused on security, privacy, and privileged user access.

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, and local law enforcement agencies 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; transmission data to and from the CJIS Division is encrypted; and firewalls are mandated and in place.

Electronically, the biometrics will be supported through the Electronic Biometric Transmission Specifications (EBTS), which currently supports fingerprint, palm print, latent 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 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 aforementioned ANSI/NIST-ITL standard provides the guidelines for the exchange of information between various federal, state, local, tribal, and international systems, the FBI's EBTS defines requirements to which agencies must adhere when electronically communicating with the FBI.

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.

Only authorized users have the ability to gain access to conduct a facial recognition search within the NGI-IPS System. System access lists are updated as personnel change job positions or leave CJIS/FBI service. The NGI-IPS provides access and authentication to system level information based upon the authorized General User (e.g., contributor) and Privileged User (system administrator) access and as defined within the NGI User's Guide. Privileged Users are provided with the capabilities to view submission data for purposes linked to NGI administration. This includes the ability to view probe photos for the purpose of troubleshooting submissions. Privileged Users lists are reviewed continuously using automation for compliance according to the IT Security Policy (DOJ-2640-E). General User lists are maintained by the CJIS Customer Service group and the CJIS Audit Unit and reviewed periodically for authorized usage. 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 approved CJIS Security Policies and vetted by the individual state and federal agency CJIS Systems Officers (CSOs).

CJIS User Agreements and Outsourcing Standards also define parameters to information sharing. Federal and State audits are performed to ensure compliance. The CSO is responsible for implementing and ensuring compliance with the CJIS Security Policy. The CJIS Division provides training assistance and up to date materials to each CSO and periodically issues informational letters to

notify authorized users of administrative changes affecting the system. CSOs at the state and federal level are responsible for the role-based training, testing, and proficiency affirmation of authorized users within their respective states/federal agencies. All users must be trained within six months of employment and biennially re-tested hereafter.

All users are subject to periodic on-site audits conducted by both a user's own oversight entity and the CJIS Division Audit Unit. The CJIS Division conducts audits on a triennial basis. The audits assess and evaluate users' compliance with CJIS technical security policies, regulations, and laws. Deficiencies identified during audits are reported to the CJIS Division Advisory Policy Board (APB). The CJIS APB operates pursuant to the Federal Advisory Committees Act and is comprised of representatives from federal, state, and local criminal justice agencies who advise the Director of the FBI regarding CJIS systems, such as the NGI-IPS. System access may be terminated for improper access, use, or dissemination of system records.

In addition, each FBI Information System Security Officer (ISSO) 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 system security authorization to operate 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 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 when criminal and civil subjects attain 110 years of age or seven years after notification of death with biometric confirmation. NARA has determined automated FBI criminal history information and NGI transaction logs are to be permanently retained. Biometrics such as photos may be removed from NGI earlier than the standard NARA retention period pursuant to a request by the submitting agency or the order of a court of competent jurisdiction.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. _X____ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

The NGI SORN is published at 81 Fed. Reg. 27, 284 (May 5, 2016); 82 Fed. Reg. 24151,156 (May 25,

2017); 84 Fed. Reg. 54,182 (October 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, preserved, and exchanged biographic and biometric information, including photos associated with criminal files, for many decades. Therefore, the Criminal Identity Group and the Unsolved Photo File of the NGI-IPS does not constitute a new collection type or collection purpose. Instead, the NGI-IPS provides the significant enhancement of facial recognition technology for these criminal photos.

The retention of more criminal photos and the searching and dissemination of these photos based on facial recognition technology presents a risk of erroneous identification. Facial recognition searching of Criminal Identity Group photos 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. In addition, the FBI is currently in the process of upgrading its facial recognition algorithm, which should garner detection rates beyond 99 percent, for all candidate list sizes. Also, in collaboration with NIST, the FBI deployed ongoing facial recognition vendor testing this past year. Traditionally, 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 facial recognition testing will enable the FBI to test its NGI-IPS facial recognition technology annually, as well as permit other vendors to submit facial recognition algorithms to NIST at least once a year.

Internally, the FBI monitors the candidate photos returned to requesters in response to search requests and works with those requesters in refining thresholds to improve the success of investigative facial searches performed in the NGI-IPS. In addition, the FBI performs regression and baseline tests on the

FBI test environments, which have been set up with data and environments that are scaled representatives of the operational environment. The FBI continuously tests and evaluates the NGI-IPS with each system change to ensure that accuracy is not negatively affected. The FBI recently designed a facial recognition test strategy in order to perform an annual facial recognition analysis of the NGI-IPS operational environment to ensure performance, accuracy, and integrity of the algorithm and the data. Within fiscal year 2020, the FBI will: define proper statistical size; identify the composition of the data set in alignment with business needs; define the operational test to ensure the integrity of both the operational environment and the projected results; develop and test any necessary test tools needed to perform the annual analysis; and, define the output for the business users for efficient reporting.

Although facial recognition 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. When authorized law enforcement users receive 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. Other indicators and factors must be considered by the submitting agency prior to making an identification. Law enforcement users are required to take facial recognition training prior to accessing the NGI-IPS, in order to conduct an effective manual review of the returned candidate photos.

Photos submitted to the NGI-IPS for retention by law enforcement agency users must meet the requirements of the Criminal Identity Group or the UPF, as described in Section 2. It is the responsibility of the participating law enforcement agencies to develop appropriate use policies for NGI-IPS facial recognition searches, 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 agency users must also ensure compliance with the CJIS Security Policy, CJIS User Agreement, and the NGI-IPS Policy and Implementation Guide. The NGI-IPS Policy and Implementation Guide expressly prohibits collection of probe photos in violation of an individual's First and Fourth Amendment rights.

The FBI made several decisions to protect privacy and civil liberties when it developed the facial recognition 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 to the Criminal Identity Group, the FBI ensured that only those photos collected pursuant to a probable cause standard and positively associated with ten-print fingerprints would be available for searching. Further, to maintain the integrity of the Criminal Identity Group, 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 law enforcement investigation and must be collected in compliance with law and policy, such photos are not retained in the NGI-IPS.

Likewise, the FBI made several decisions to protect privacy and civil liberties in its development of the Unsolved Photo File. 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.

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 NGI mitigate this risk. The FBI CJIS Audit Unit continues to conduct audits of federal, state, and local 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 processes and provide 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 audits.

The increased retention and searching of photos in the NGI-IPS presents 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 purposes or to unauthorized recipients. Another privacy risk could be the improper access to the data or misuse of information in the system, such as unauthorized electronic searching of the criminal and civil photos. These risks are mitigated through NGI'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 CJIS Division has an established Audit Unit that regularly visits agencies that are authorized to collect and submit photos. Allegations of misuse of CJIS systems, including NGI, 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. Additionally, the privacy risk is mitigated because 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. This risk is further mitigated to the extent that an agency that contributes information to NGI has a process in place for access to or correction of the contributing agency's source records.