Federal Bureau of Investigation

Privacy Impact Assessment
for the
[Next Generation Identification Iris Service]

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: [October 29, 2020]

(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) addresses the Federal Bureau of Investigation's (FBI's) Next Generation Identification Iris Service (NGI-IS) which will replace the FBI's current iris pilot.[1] The NGI-IS will consist of a national iris repository that resides in the FBI's NGI system and an iris search capability for authorized users. The NGI system serves as the FBI's biometric identity and criminal history records system[2] and maintains individuals' fingerprints and associated identity information submitted to the FBI for authorized criminal justice, national security, and civil purposes. The NGI-IS will permit authorized criminal justice agencies to enroll iris images along with new criminal history records, or to append iris images to existing criminal history records. In addition, the authorized criminal justice agencies may search iris images against those enrolled in the national repository to assist with criminal identifications. These authorized agencies include local, state, tribal, and federal law enforcement agencies and agencies directly engaged in the administration of criminal justice functions, such as prosecution, probation, parole, and corrections.

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 FBI has conducted an iris pilot with approximately sixteen partner agencies for the past several years. During the course of this pilot, the FBI has determined that iris recognition offers a highly accurate and rapid biometric identification option for criminal justice agencies. Iris recognition technology is an automated process of identifying individuals by their iris patterns (the iris is the colored part of the eye) with the use of mathematical algorithms and near-infrared cameras designed to specifically collect iris images. Each iris contains a unique pattern of ridges and folds that are specific to an individual. The FBI works closely with the National Institute of Standards and Technology (NIST) to determine accuracy levels of various biometrics. NIST has performed multiple tests to determine that the iris recognition technology used by FBI in this program is an accurate and dependable means of identification.[3]

The FBI has obtained over 1.8 million iris images that will form the foundation of the NGI-IS repository. The NGI-IS will contain iris images from local, state, tribal, and federal partners obtained during arrest, a subsequent criminal proceeding, incarceration, or post-trial release. The iris images

[1] *See* Iris Pilot PIA at www.fbi.gov/services/information-management/foipa/privacy-impact-assessments.
[2] See NGI System of Records Notice, 81 Fed. Reg. 29,284 (May 5, 2016); 84 Fed. Reg. 54,182 (October 9, 2019).
[3] See http://pages.nist.gov/IREX10/

obtained using a near-infrared camera may be submitted by criminal justice agencies for criminal justice purposes, in bulk or single transactions. Iris images submitted for retention, as opposed to for searching purposes, must be associated with ten-print criminal fingerprints and/or a Universal Control Number (UCN), which is a unique numeric identifier in NGI. The iris images may be submitted at the same time as the establishment of a criminal identity in NGI; or they may be submitted to augment the record after a criminal identity has been established.

The FBI will also permit authorized criminal justice agencies to search iris images against iris images maintained in the NGI-IS. A search must consist of a separate iris image of each eye captured by a near-infrared iris camera in a controlled setting. Examples of the use of iris identification searches include: by correctional facilities to monitor the entry, exit, and release of prisoners; by supervised release offices for the automatic check-in of parolees, probationers, and sex offenders; and by the Department of Homeland Security to ensure more effective border protection and officer safety. Iris images submitted for searching are not retained in the NGI-IS repository nor are they appended to any existing criminal history records.

The iris search is performed "lights-out", without human intervention, and the submitting agency will receive an identification or a no identification result. For identification searches, a search that results in a score better than a predetermined match threshold is deemed a match. There is no standard which prescribes match score thresholds for biometric algorithms. The FBI takes responsibility for determining settings for match score thresholds, to which several factors contribute. These factors include, but are not limited to: NIST test and evaluation findings, FBI test and evaluation findings, operational testing (e.g. pilot deployments, prior algorithms used), and vendor recommendations. NIST has evaluated the iris algorithm developed by the FBI's iris algorithm vendor, and currently this vendor's algorithm is in first place on the NIST accuracy leaderboard. The FBI performed its own test and evaluation on the actual iris algorithm deployed in NGI, to which very similar accuracy results were obtained. The FBI also benefited from piloting iris recognition in an operational environment with multiple federal and state law enforcement agencies across the nation for seven years prior to iris deployment within NGI. Data collected from the pilot as well as direct feedback from FBI law enforcement partners all contributed to the identification of an appropriate match score threshold. Prior to operational deployment in NGI, the FBI spent months performing internal testing in a non-operational environment to confirm the iris algorithm performed as intended with regard to function and results.

Only one match will be returned to the submitting agency, with a caveat that the response is based on a search of the NGI-IS repository and does not preclude a record from existing in other biometric or biographic repositories. All iris image match responses include, but are not limited to, the subject's name, UCN, and a mugshot if available. The submitting agency also may choose to receive the subject's associated criminal history record information (CHRI). In addition to criminal events, the CHRI includes biographic information, such as name, date of birth, place of birth, gender, race, and social security number.

If an iris image match occurs in the NGI-IS, an automated query of the National Crime Information Center (NCIC) system will be performed with the use of a unique identifier. The unique identifier positively links the same identity in NGI and NCIC. NCIC is a biographic crime data system that supports law enforcement nationwide with, among other things, identifying and locating wanted persons, missing persons, fugitives, sex offenders, and gang members. Any NCIC response returned

in response to an iris match will contain additional biographic and law enforcement information related to the subject. The results will include a list of identifiers and case numbers for each NCIC file that contains the subject's identity (e.g., wants/warrants, sex offenders). The NCIC response can also contain caution and medical codes, and handling caveats when available. If an active want/warrant is found, the offense (e.g. parole violation), original offense (e.g. assault), and wanting agency are included in the iris response.

In addition to the iris images maintained in the NGI-IS, the FBI receives iris images typically associated with other biometrics, such as fingerprints and photos, from federal and foreign partners. The FBI retains these iris images in accordance with its law enforcement and national security missions, and the majority of the images are obtained from non-U.S. persons. To the extent that these iris images are not collected pursuant to the evidentiary threshold (i.e. arrest, a subsequent criminal proceeding, incarceration, or post-trial release) described in this PIA, they are not processed according to the policy requirements within this PIA. Separate policy and privacy documentation will be prepared for these iris images, as appropriate.

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); USA PATRIOT ACT of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001)
X	Executive Order	8781, 8914, 10450
X	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)	

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.

Iris images submitted for enrollment in the NGI-IS must be submitted with criminal ten-print fingerprints or a UCN to ensure positive identification. If the iris images are submitted concurrent

with an arrest, the criminal history information will include biographic information such as name, date of birth, place of birth, and social security number. A search of the NGI-IS requires only the submission of the iris images. If an identification match occurs, additional biographic, biometric, and criminal history information may be returned to the requesting criminal justice agency.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	C, D	
Date of birth or age	X	C, D	
Place of birth	X	C, D	
Gender	X	C, D	
Race, ethnicity or citizenship	X	C, D	
Religion	X	C, D	
Social Security Number (full, last 4 digits or otherwise truncated)	X	C, D	
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			

(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
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C, D	
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	C, D	
- **Video containing biometric data**			
- **Fingerprints**	X	C, D	
- **Palm prints**			
- **Iris image**	X	C, D	
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	
- **User passwords/codes**			
- **IP address**	X	A	
- **Date/time of access**	X	A	
- **Queries run**	X	A	
- **Content of files accessed/reviewed**	X	A	
- **Contents of files**	X	A	
Other (please list the type of info and describe as completely as possible):			

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

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

Government sources:					
Within the Component	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)			
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			Iris search responses will be shared via an NGI electronic connection. Only identity information associated with a positive match will be returned.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
DOJ Components	X			Iris search responses will be shared via an NGI electronic connection for all authorized criminal justice agencies. Only identity information associated with a positive match will be returned.
Federal entities	X			See above.
State, local, tribal gov't entities	X			See above.
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 iris images maintained in the NGI-IS may be used for FBI research and development purposes in accordance with applicable federal law and regulations. When the FBI provides data to NIST, it is subject to strict security and use protections pursuant to an interagency agreement between the FBI and NIST. Additional protections are delineated in "Government Furnished Information" letters which the FBI provides to NIST regarding specific research projects and data sets. Any iris image used for research and development would be sent without personally identifiable information, such as name, 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 iris image if required by the specific research activity. The data is encrypted by the FBI in accordance with Federal Information Processing Standards (FIPS) 140-2 requirements prior to release to NIST. The data is stored in FBI 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 data. No iris images are released to the public for "open data" purposes.

Section 5: Notice, Consent, Access, and Amendment

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

No Privacy Act notice is provided to individuals regarding the collection, use, and sharing of their iris images in the NGI-IS repository. The FBI has exempted itself from the requirement of 552a(e)(3) for the criminal records maintained in NGI. However, the iris images are collected in conjunction with ten-print fingerprints upon arrest or in other custodial situations 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 iris images and the most current version may be found at 84 Fed. Reg. 54,182 (October 9, 2019). This PIA also provides general notice, as does the previously published PIAs regarding NGI, which may be found at https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments.

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

A person under arrest or incarcerated may have no opportunity to refuse the collection of biometrics. Nevertheless, federal agency criminal or national security uses of the information in the NGI system must comply with the provisions of applicable law, including the Privacy Act, if applicable.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Title 28 CFR part 16, subpart A, provides general guidance on access to information in FBI files pursuant to the Freedom of Information Act; and 28 CFR part 16, subpart D, provides general guidance regarding access to, and amendment of, information in FBI files pursuant to the Privacy Act. Title 28 CFR 16.30-16.34 establish specific procedures for an individual to obtain a copy of his or her criminal history record from the NGI System for review and correction. Note, however, that the FBI maintains exemptions from access and amendment provisions of the Privacy Act for certain records maintained in 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).

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):** October 27, 2018, within the Next Generation Identification (NGI) System. **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	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The NGI system, including the Iris Service, 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 Criminal Justice Information Services (CJIS) enterprise system audit consolidation and monitored for irregular activities or compliance failures.
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**.
	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:

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 (including iris images) 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 criminal justice 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 iris images will be supported through the Electronic Biometric Transmission Specifications (EBTS), which currently supports fingerprint, palm print, latent print, face photos, 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 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.[4] Agencies wishing to enroll and search iris images in the NGI-IS may confirm their compliance with EBTS by submitting test data to NGI's operational testing environment before proceeding with full operational capability. This testing permits CJIS and its users to identify and resolve any issues before information is disseminated in the live environment.

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.

Specific to the NGI-IS, users must adhere to policy and technical requirements promulgated in the Iris Service Policy and Implementation Guide. This Guide advises authorized users that only iris images collected pursuant to criminal justice purposes may be enrolled in and searched against the NGI-IS. It provides specific quality control requirements and acceptable enrollment methods to ensure that iris images are associated with the correct identities. It also provides best practices for iris image capture to ensure quality of data. Finally, the Guide provides specific technical requirements for connection to the NGI-IS to ensure security and integrity of the data.

Only authorized criminal justice users may enroll iris images or conduct an iris search within the NGI-IS. NGI provides access and authentication to its data based upon the authorized General User (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 capability does not include the ability to view iris images submitted for searching. 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

[4] See https://www.fbibiospecs.cjis.gov

with the NGI records retention schedule. General Users of NGI 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 to information sharing. Federal and State audits are performed on a triennial basis 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 state or federal agencies. At a minimum, the training and testing must meet the requirements of the CJIS Security Policy; state and federal users may impose additional requirements as needed. All users must be trained within six months of employment and biennially re-tested hereafter.

The CJIS systems are not available to users unless there has been an application for, and assignment of, an Originating Agency Identifier (ORI), a unique number assigned to each using entity. 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 CJIS. State and federal CSOs must apply to the CJIS Division for the assignment of ORIs and CJIS staff evaluates these requests to ensure the agency or entity meets the criteria for the specific type of ORI requested. CJIS maintains an index of ORIs and logs each dissemination of identification records to the applicable ORI.

All users are subject to periodic on-site audits conducted by both a user's own oversight entity and the CJIS Division Audit Unit. Both the user agency and the CJIS audits must occur, at a minimum, on a triennial basis. Audits typically occur as scheduled, but may be requested at other times if a compliance issue is identified. The audits conducted by CJIS review all uses of NGI, and the new Iris Service will become an additional component of these audits. The audits assess and evaluate users' compliance with CJIS 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 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 NGI. 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 security certification and accreditation process. All FBI employee and contractor personnel must complete privacy training and annual information security training. The training addresses the roles and responsibilities of the users of FBI systems, and raises awareness of the sensitivity of the information contained therein and how it must be handled to protect privacy and civil liberties.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

The National Archives and Records Administration (NARA) has approved the destruction of fingerprint cards and associated information, including other biometrics, when criminal and civil subjects attain 110 years of age. NARA has determined automated FBI criminal history information and NGI transaction logs are to be permanently retained. Biometrics, including iris images, and associated biographic information 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 (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, preserved, and exchanged biographic and biometric information for many decades. The Integrated Automated Fingerprint Identification System (IAFIS), the predecessor system to NGI, was enhanced to store iris images in 2009. Between 2009 and the 2013 launch of the FBI iris pilot, approximately 30,000 iris enrollments were submitted to the

IAFIS. During the FBI iris pilot, the iris repository grew to over 1.8 million images. The NGI-IS provides the significant enhancement of iris recognition technology for improving automated searches of these iris images. The FBI accepts iris images for enrollment or searching from authorized criminal justice agencies that currently comply with all NGI system requirements. The FBI provides iris search results to only those same criminal justice agencies.

As with most biometric searches, there is a risk of misidentification. The FBI recognizes that any new biometric capability must be carefully assessed and tested prior to implementation to ensure sufficient reliability and minimum error. This has been accomplished over the past several years by the successful deployment and utilization of the FBI iris pilot. Additionally, regular updates to iris technology continually improve its accuracy, further reducing the risk of misidentification.

The primary and preferred enrollment method for iris images is a criminal ten-print submission with two iris records attached. The accompanying ten-print fingerprints serve to positively link the iris images to a single identity. Another potential risk of misidentification may occur when the iris images are submitted to the NGI-IS without accompanying ten-print fingerprints. Iris images may also be submitted after a criminal identity record has already been established in NGI if the iris images are positively associated with a UCN. This policy permits the enrollment of iris images (either to supplement a single record or in bulk) to augment criminal history records that already reside within NGI. However, each distinct UCN is tied to a single identity positively identified by fingerprints, mitigating the risk of misidentification. Submissions with non-existing or invalid UCNs will be rejected by NGI. If the FBI receives a valid UCN, but one that does not belong to the subject of the iris image because the contributor has assigned the UCN to the wrong person, the accompanying iris images may be associated with the wrong identity. To mitigate this risk, the FBI has established an NGI-IS Policy and Implementation Guide that requires all submitters to verify all criminal iris images match the UCN, as well as other unique identifying information and the appropriate arrest cycle, prior to submission to the CJIS Division. The risk is further reduced by both state and federal audits that ensure accuracy. The CJIS Security Policy requires audits by federal and state partners and these agencies must have policies in place to show compliance with the requirements of the CJIS Security Policy. The CJIS Security Policy's information security requirements and controls include security training, reporting of security incidents, access control, media protection, and physical and personnel security. The FBI therefore expects such situations will be rare, and any such erroneous association would be quickly discovered and corrected via comparisons with text-based descriptors and/or photos of the subject, or with positive fingerprint identification.

There may be a privacy risk that using an incoming iris image to generate a text-based query of NCIC might not be sufficiently reliable to produce an appropriate NCIC response, thereby either missing records in NCIC or returning another subject's NCIC records. To mitigate this risk, all cascaded NCIC searches are accomplished by using a unique identifier from the biometric record, so that any NCIC responses will be linked by a unique identifier established from positive biometric identification. Although there remains the risk of erroneous UCN linkage resulting from human error, system failure, or data corruption, this risk is considered extremely small because of CJIS system maintenance standards and audits conducted by state agencies and the CJIS Division. The risk of erroneous linkage is also mitigated by the caveat provided with all iris responses and other policy and security requirements placed on the users. The caveat informs authorized users that "This response is based on a search of the NGI Iris Service repository and does not preclude a record from existing in other biometric or biographic repositories". In this way, the criminal justice users of the NGI-IS are

advised that they should conduct their standard investigatory practices and not rely solely on the response from the NGI-IS.

The increased retention and searching of iris images by the NGI-IS will present a privacy risk that the iris images will be accessed or searched without authorization or used for purposes unknown to the agency that provided the image. The increased number of iris images that are retained and searched may also create a risk that iris images will be disseminated for unauthorized purposes, or to unauthorized recipients. However, the NGI-IS will use existing robust NGI system security requirements and FBI user rules regarding access and dissemination. Dissemination of information is linked to the authorized user and the agency that requested the information. Additionally, the system stores information regarding dissemination of iris images, such as date, time, and requester in audit logs. Such risks are also mitigated through training and by periodic audits conducted by the FBI to ensure system searches are relevant and necessary to the person's official duties. The CJIS Division has an established Audit Unit that regularly visits and reviews implementation of FBI requirements by entities that are authorized to collect and submit iris images in an effort to ensure all requirements are being implemented. Allegations of misuse of CJIS systems, including NGI, are generally referred to the appropriate state or federal agency CSO of the jurisdiction where the misuse occurred, and the FBI responds to all such allegations. For those occasions when records maintained in the NGI are improperly accessed or disseminated, the CJIS APB has an established Sanction Committee to address misuse.

Additionally, the risk of any misuse of the information is further mitigated by the FBI User Agreement and the CJIS Security Policy. The User Agreement specifies the ways in which each agency—CJIS and each user agency—is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security; dissemination and logging; and security of criminal history records. Additionally, each state or federal agency shall be responsible for maintaining the integrity of the system in accordance with the CJIS Security Policy, as well as any additional agency policy to ensure only authorized terminal access; only authorized transaction submission; and proper handling and dissemination of CJIS data. Each agency, enrolling or searching iris images, shall also be responsible for computer security incident reporting as required by the CJIS Security Policy.

The privacy risk of maintaining erroneous iris images or information associated with iris images is further mitigated by the actions taken by the FBI, in compliance with law and policy, to ensure the accuracy of the information in the NGI-IS. The FBI takes action to correct any erroneous information of which it may become aware and has established policies and technical safeguards to both prevent inaccurate information from entering the system and to conduct ongoing reviews of the information residing in the system. Additionally, the maintenance and dissemination of information must comply with the provisions of any applicable law, regulation, or policy, including the Privacy Act of 1974. Among other requirements, the Privacy Act obligates the FBI to make reasonable efforts to ensure the information it disseminates to non-federal agencies is accurate, complete, timely, and relevant. Privacy risks are further reduced to the extent that agencies that contribute information also have processes in place for access to or correction of their source records.