Federal Bureau of Investigation

Privacy Impact Assessment
for the
FBI Iris Pilot

Issued by:
Ernest J. Babcock, Privacy and Civil Liberties Officer

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

Date approved: April 21, 2017

(May 2015 DOJ PIA Form)

EXECUTIVE SUMMARY

This Privacy Impact Assessment (PIA) addresses the FBI Iris Pilot (IP) which allows authorized criminal justice agencies to enroll iris images with criminal records or append iris images to existing criminal records. These enrolled iris images may then be searched using probe iris images submitted by authorized criminal justice agencies to assist with criminal identifications. Iris recognition offers a highly accurate, contactless, and rapid biometric identification option for criminal justice agencies. The FBI IP enables the evaluation of iris technology in an operational setting while simultaneously addressing key challenges associated with large-scale, criminal justice application. The FBI IP provides the opportunity to build and establish a national iris image repository; ascertain technical and operational best practices; develop standards for iris capture and transmission; and ensure that privacy and civil liberties protections are integral to the service.

Section 1: Description of the Information System

The FBI relies on its partnerships with local, state, tribal, and federal agencies to collaboratively choose new technologies that would best serve the law enforcement and criminal justice communities. Iris recognition technology is becoming a part of everyday operations for a number of state and local law enforcement agencies and correctional institutions. Iris recognition systems have been deployed in local jurisdictions to identify subjects who have been arrested and who are transferred within or between correctional facilities. As more agencies adopt the iris as a viable means of identification, the FBI has recognized the need for a national iris repository and search capability.

FBI efforts to utilize iris recognition began with gathering technical and funcational requriements from anticipated system users for the Criminal Justice Information Services (CJIS) Division Next Generation Identification (NGI) system[1]. CJIS's criminal justice partners requested iris recognition as an additional biometric service, which led to a planned iris pilot. The FBI IP was initially scheduled for approximately 12 to 18 months to offer iris recognition services to select criminal justice partners. However, the CJIS Division has decided to continue the IP for an estimated two to three years. Participating agencies may enroll iris images with arrest transactions[2] and perform identification searches of all enrolled iris images.

At the start of the FBI IP, the CJIS Division retained approximately 30,000 iris images collected largely by the FBI and its federal partners. It now retains approximately 450,000 enrollments. The FBI IP repository contains images from local, state, tribal, and federal databases obtained during criminal bookings, incarceration, or other criminal justice proceedings. The iris images may be submitted in bulk or single transmissions, and images submitted for retention are associated with tenprint

[1] NGI is the FBI's system for the exchange of fingerprints and associated criminal history record information. NGI also includes other biometrics, such as latent fingerprints, palmprints, and mugshots.
[2] In order for iris images to be accepted, they must either be connected with a tenprint fingerprint set and/or a unique numeric identifier.

fingerprints and/or a unique numeric identifier. In addition to the iris images and numeric identifiers, the FBI IP also maintains some of the biographic data (*e.g.* sex, race, age) collected with the tenprint fingerprint submission.

The FBI IP permits authorized criminal justice agencies to search iris images against the FBI IP repository. 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. These agencies are required to execute a Memorandum of Understanding (MOU) with the FBI for participation in the FBI IP.

Iris recognition technology is the process of identifying individuals by their iris patterns with the use of software and cameras designed to specifically collect iris images. Algorithms use the intricate structures and detail of the iris image to conduct automated matching. It is recommended that agencies submit images of both irises of an individual, although the technology accurately searches a single iris image. There are 2 types of iris image searches: (1) identification and (2) investigative. Identification searches are performed for the authorized agencies when the iris image submitted is of high quality (i.e. the image is captured by an 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 homeland security to ensure more effective border protection and officer safety.

For identification searches, a search that results in a score better than a predetermined match threshold[3] is deemed a match. Presuming there are quality images, it is highly unlikely that an identification search will result in more than one candidate. All iris image match responses include, but are not limited to, the subject's name, unique numeric identifier, and mugshot if available. If an iris image match occurs as a result of an identification search, the subject's biographic information is cascaded against the National Crime Information Center (NCIC) and the Interstate Identification Index (i.e. the name index for NGI) to locate any additional identifiers, relevant law enforcement action, and criminal history record information. Although the accuracy of iris identification is now considered to be comparable to fingerprint identification, the FBI IP still returns all iris image matches to the authorized criminal justice agencies with a caveat that cautions the criminal justice agency that records may exist in other biometric or name based repositories and that additional law enforcement action should not be based solely on the IP match.

Investigative searches of the iris repository are currently performed on a very limited basis. Investigative searches are performed when lesser quality "unknown" iris images are submitted for searching against the "known" repository of iris images. An investigative search is designed to return up to 50 match candidates. The FBI IP allows a user to apply search parameters by biographic and/or

---

[3] Biometric algorithms use "match scores" when comparing samples. A match score can be thought of as a similarity score; the higher the number, the higher the likelihood of a match. Match scores are vendor specific and proprietary, making little sense to other vendors or the general public. Nevertheless, a predetermined match threshold is a match score number at which a vendor is able to conclude that a match has occurred when comparing samples.

demographic data to limit investigative search responses. Investigative responses include a caveat that cautions the criminal justice agency that users should not rely solely on the investigative search responses as the impetus for any law enforcement action and true identities must be independently verified.

The FBI IP functions as a stand-alone/auxiliary computer environment that has no direct connection with the NGI system but uses automated routing for necessary information sharing between the systems. If an agency enrolls its iris images in "bulk" (i.e. the images are associated with unique identifying numbers) the images are retained only in the IP repository. They are not added to or otherwise retained in NGI identity records. If an agency enrolls "live" iris images (i.e. the images are associated with criminal tenprint fingerprints) the images are retained only in the IP repository; however, the existence of iris images will be documented in the appropriate NGI identity records. An incoming iris search submission's active presence in the NGI system will be transitory, lasting only for the few seconds needed for the iris search itself (including any cascaded NCIC search).

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security	X	Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID	X	Credit card			
Other identifying numbers (specify): This data is obtained from the tenprint fingerprint submission associated with the iris image. Identifying numbers may include a Universal Control Number (UCN)[4] and/or a State Identification Number (SID)					

General personal data					
Name	X	Date of birth	X	Religion	
Maiden name		Place of birth	X	Financial info	
Alias	X	Home address		Medical information	
Gender	X	Telephone number		Military service	
Age	X	Email address		Physical characteristics	X
Race/ethnicity	X	Education		Mother's maiden name	

[4] A UCN is a unique identifying number used to index an individual's criminal or civil identity record in NGI.

General personal data
Other general personal data (specify): This data is obtained from the tenprint fingerprint submission associated with the iris image.

Work-related data					
Occupation		Telephone number		Salary	
Job title		Email address		Work history	
Work address		Business associates			
Other work-related data (specify):					

Distinguishing features/Biometrics					
Fingerprints		Photos	X	DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	X
Voice recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify):					

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	X
IP address	X	Queries run	X	Contents of files	X
Other system/audit data (specify):					

Other information (specify)

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax		Online	
Telephone		Email			
Other (specify): The CJIS Division does not obtain iris images directly from an individual. The FBI IP is populated with iris images collected by criminal justice agency partners.					

Government sources					
Within the Component	X	Other DOJ components	X	Other federal entities	X

State, local, tribal	X	Foreign			
Other (specify): Iris images are collected and submitted to the CJIS Division by authorized criminal justice agencies in accordance with their lawful missions.					

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

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

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 Iris Pilot launch, approximately 30,000 iris enrollments were submitted to IAFIS. Therefore, the FBI IP does not constitute a new collection type or collection purpose. Instead, the FBI IP provides the significant enhancement of iris recognition technology for automated searching of these iris images.

As with most biometric searches, there is a risk of misidentification. More specifically, there is arisk that the technology may not be sufficiently reliable to accurately locate other iris images of the same identity, resulting in an unacceptable percentage of misidentifications. The FBI recognizes that any new biometric capability must be carefully assessed and tested prior to implementation to ensure sufficient reliability and minimum error. Based on current technology, iris recognition is incredibly accurate and possesses the ability to perform matches at thresholds considered acceptable for national or international identification systems. Regular updates to the technology continually increase the accuracy of the tool, further reducing the risk of misidentification.

In 2012, the National Institute of Standards and Technology (NIST) published a report on the evaluation of large-scale one-to-many iris identification algorithms. This report, entitled NIST IREX III, was an independent and public test of iris identification search technologies. It used millions of images to validate results published in academic literature that iris is a very powerful biometric and clearly affirmed the potential for iris recognition to accomplish large-scale identity management tasks. Results from this report were leveraged to select the best iris identification algorithm for the FBI IP. The selected algorithm had an impressive rank-based accuracy performance of 98.4% True Positive Identification Rate using a single iris image and the use of a second iris image from the subject's other eye increases the accuracy to over 99%. The full IREX III report may be found at

http://www.nist.gov/itl/iad/ig/irexiii.cfm. With iris recognition algorithms now embedded within the FBI IP, the technology can be further evaluated for accuracy.

As discussed above, the FBI IP returns all iris image matches to the authorized criminal justice agencies with the appropriate caveat that cautions the criminal justice agency that records may exist in other biometric or name-based repositories and that additional law enforcement action should not be based solely on the FBI IP match. Additionally, the risk of any misuse of the information is further mitigated by the MOU emphasizing that information derived from the FBI IP search requests and responses shall only be used as investigative leads and shall not be considered as positive identifications. The parties are prohibited from relying solely on IP search responses as the sole impetus for law enforcement action. The MOU also includes provisions emphasizing that all CJIS policies regarding access to and use of CJIS information apply, including compliance with the CJIS Security Policy.[5] Finally, the FBI's standard MOU states that FBI IP information may identify United States persons, whose information is protected by the Privacy Act of 1974 and all such information should be handled lawfully pursuant to the provisions thereof. It is the responsibility of the participating criminal justice agencies to comply with their state privacy laws and to develop appropriate use policies for FBI IP iris recognition results, in accordance with the applicable laws and policies of their relevant governmental jurisdictions.

There may be a 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 related records in NCIC or returning another subject's NCIC records. To mitigate this risk, all cascaded NCIC searches are accomplished by using the UCN 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. This risk of erroneous linkage is also mitigated by the caveat provided with all iris responses and the guidance provided in the MOU as described in this section above.

Another potential risk stems from the fact that criminal iris images may be submitted without accompanying tenprint fingerprints in bulk format during the pilot. Accompanying tenprint fingerprints serve to tie iris images to a single identity positively confirmed by the fingerprints. The primary and preferred enrollment method for iris images is the Criminal Tenprint Submission (CAR/CNA) with two iris records attached. During the FBI IP however, iris images may be submitted with reference to an existing UCN and/or a numeric identifier.

Regarding identification based on UCN, each UCN is tied to a single identity positively identified by fingerprints. Submissions with nonexisting or invalid identifying numbers will be rejected by the system. However, the submitting agency may not use the correct UCN for the subject of the iris submission, or the wrong UCN may be submitted due to typographical, clerical, or other error. If the FBI receives a valid UCN, but one that does not belong to the subject of the iris image, the accompanying iris images may be associated with the wrong identity. To mitigate this risk, the FBI has executed agreements with submitters of bulk iris images without accompanying tenprints. The agreements require that a submitter verify that all criminal iris images match the UCN, State

[5] *See* https:www.fbi.gov/services/cjis/cjis-security-policy-resource-center

Identification Number (SID), and/or Miscellaneous Number (MNU) and arrest cycle prior to submission to the CJIS Division. If the UCN is known, the FBI requests that the UCN be provided, solely or in addition to, the SID and/or MNU. This risk is further reduced by both state and federal audits that ensure accuracy. The FBI therefore expects that 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.

The privacy risk of maintaining erroneous iris images or information associated with iris images is further mitigated by the FBI's substantial interest in ensuring the accuracy of the information in the system. The FBI takes action to correct any erroneous information of which it may become aware. Additionally, the 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 of 1974. 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. 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.

The increased retention and searching of iris images by the FBI IP presents a privacy risk that the iris images will be accessed or searched without authorization, or used for purposes unknown to the individual who provided the image. The increased number of iris images that are retained and searched, may also create a risk that the iris images will be disseminated for unauthorized purposes, or to unauthorized recipients. However, the IP uses the existing robust NGI system security requirements and user rules regarding access and dissemination. Such risks are mitigated through training and by periodic audits conducted by the FBI to ensure that system searches are relevant and necessary to the person's official duties. CJIS has an established Audit Unit that regularly visits entities that are authorized to collect and submit iris images in an effort to ensure all legislative and agency policy protections are being implemented. Allegations of misuse of CJIS systems, including NGI, are generally referred to the appropriate CJIS Systems Officer (CSO) of the jurisdiction where the misuse occurred, and the FBI responds to all such allegations. For those occasions when records maintained in NGI are improperly accessed or disseminated, both the CJIS Advisory Policy Board (APB) and the National Crime Prevention and Privacy Compact Council (Compact Council) [6] have established Sanction Committees to address the possible misuse. Dissemination of information is linked to the authorized user and the agency that requested the information. The system also stores information regarding the dissemination of iris images and related information in audit logs.

[6] The CJIS APB operates pursuant to the Federal Advisory Committees Act and advises CJIS on the criminal justice uses of its systems, including NGI. The Compact Council was established pursuant to statute and facilitates the exchange of authorized interstate criminal history records for noncriminal justice purposes.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
X	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities		For administrative matters
X	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
X	Other (specify): probation, parole, corrections		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

As listed in Section 3.3, the FBI has statutory authority to collect, preserve, and exchange biographic and biometric information for criminal, civil, and national security purposes. Pursuant to that authority, CJIS's mission is to reduce terrorist and criminal activities by improving and expanding biometric identification and criminal history information services. The FBI IP will have a direct impact on the criminal justice community by assisting in the disruption and deterrence of criminal activity and terrorism by providing local, state, tribal, and federal criminal justice agencies with a fast, accurate, and contactless biometric identification service to identify wanted persons, gang members, sex offenders, and others. Increasing the number of iris images in the FBI IP will enhance this capability and expand the usefulness of this biometric.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

Authority		Citation/Reference
X	Statute	28 U.S.C. §§ 533, 534; 42 U.S.C. § 3771; 44 U.S.C. §3301; USA PATRIOT ACT of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).
X	Executive Order	Executive Orders 8781, 8914, and 10450
X	Federal Regulation	28 CFR 0.85, 20.31, 20.33

	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

3.4 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, or seven years after notification of death with biometric confirmation. NARA has determined automated FBI criminal history information and NGI and NCIC transaction logs are to be permanently retained. Biometrics 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. Chronological records of iris image searches and responses will be permanently retained in the respective NGI and NCIC transaction logs.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.) In addition to providing a narrative answer, please consult the ISSO/ISSM for the system's NIST 800-122 PII Confidentiality Safeguard Security Controls.

PII Confidentiality Risk Level:

☐ **Low** ☐ **Moderate** ☑ **High**

- Is the system protected as classified; or
- Does the system involve intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system; or
- Is the system critical to the direct fulfillment of military or intelligence missions (excluding routine business or administrative applications, e.g., finance, logistics, personnel management)?

☐ **Yes** ☑ **No**

If Yes, the system meets the NIST 800-59 definition of a National Security System.

Access controls

X	Access Enforcement: the system employs role-based access controls and enforcement mechanisms for PII.
X	Separation of Duties: users of de-identified PII data are not also in roles that permit them to access the information needed to re-identify the records.
X	Least Privilege: user roles enforce the most restrictive set of rights/roles for each user group.
X	Remote Access: remote access is prohibited or limited to encrypted communication channels.
X	User-Based Collaboration and Information Sharing: automated mechanisms are in place for matching access authorizations to contractual/MOU/MOA restrictions.
X	User-Based Collaboration and Information Sharing: automated mechanisms are in place for matching PII access authorizations to access restrictions, such as contractual/MOU/MOA requirements. Access Control for Mobile Devices: data can only be accessed on mobile devices that are properly secured and regularly scanned for malware.
X Access Control for Mobile Devices: data can only be accessed on mobile devices that are properly secured and regularly scanned for malware.	

Audit controls

X	Auditable Events: access to PII is audited for unauthorized access
X	Audit Review, Analysis, and Reporting: audit records are regularly reviewed for inappropriate or unusual activity affecting PII; such activity is investigated and reported; and responsive action and appropriate mitigation is taken.

Identification and Authentication controls

X	Identification and Authentication: users are uniquely identified before accessing PII; remote access requires 2-factor authentication and 30-minute "time-out" functionality.

Media controls

X	Media Access: access to system media (CDs, USB flash drives, backup tapes) is restricted.
X	Media Marking: media containing PII is labeled.
X	Media Storage: media containing PII is securely stored.
X	Media Transport: media is encrypted and stored in a locked container during transport.
X	Media Sanitation: media is sanitized prior to re-use.

Data Confidentiality controls

X	Transmission Confidentiality: information is encrypted prior to transmission or encrypted transmission is used.
X	Protection of Information at Rest: information stored on a secondary storage device (hard drive or backup tape is encrypted.

Information System Monitoring

X	Information System Monitoring: network boundaries are automatically monitored for unusual or suspicious transfers or events.

The routing of iris images to CJIS follows the standard CJIS business model where local agencies submit to a CJIS Systems Agency (CSA) or State Identification Bureau (SIB) and the CSA/SIB submits the transactions to CJIS. To participate in the FBI IP, authorized criminal justice agencies transmit their iris images over the CJIS Wide Area Network (WAN) or via a Virtual Private Network (VPN) for routing images to the stand-alone repository. Iris matches are returned to the agencies in the same manner. The CJIS WAN is used for connectivity to NGI and to authenticate with NGI. Upon successful authentication with NGI, iris image transactions are forwarded to the FBI IP, which re-authenticates the user. The FBI IP follows CJIS precedent and uses Simple Mail Transfer Protocol (SMTP) and traditional/native Electronic Biometric Transmission Specification (EBTS)[7] files for communication.

This architecture dictates that the retention and searching of iris images described in this PIA are subject to the same comprehensive security protections, access limitations, and quality control standards already in existence for NGI. Access to NGI is controlled through extensive, long-standing user identification and authentication procedures. Stringent processes are in place to ensure that only authorized users have access to the system, and the information is verified through audit logs detailing an authorized user's or agency's search and retrieval of the biometric data. The CJIS Division Audit Unit conducts periodic internal and external on-site audits of user agencies to assess and evaluate compliance with the CJIS Division Security Policy and applicable laws. Agencies requesting and receiving biometric identifications will be trained by the CJIS Systems Agency, which has overall responsibility for the administration and usage of the CJIS programs that operate in a particular state.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component		X	X	
DOJ components		X	X	
Federal entities		X	X	
State, local, tribal gov't entities		X	X	
Public				
Private sector				
Foreign governments				

[7] *See* https://www.fbibiospecs.cjis.gov

Foreign entities				
Other (specify):				

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.) [In answering the question, you should discuss user authentication, data encryption, and NIST Confidentiality Safeguard Controls.]

The criminal identity iris images are available to Department of Justice (DOJ) components when there is a need for the information in order to perform official duties, pursuant to 28 U.S.C. § 534 and the Privacy Act of 1974, 5 U.S.C.§ 552a(b)(1). Information is disclosed only to DOJ users who have been authorized access to the information. The iris images will also be shared with local, state, tribal, and federal agencies for criminal justice initiatives and national security matters as permitted by federal and state statutes, federal executive orders, or regulation or order by the Attorney General. The FBI IP will maintain information provided only by authorized agencies, which are responsible for ensuring that accurate and complete biographic and biometric information is submitted in accordance with CJIS data quality standards and operating policies.

Additionally, the FBI enters into Memoranda of Understanding (MOUs) with state and federal agencies prior to allowing access to the FBI IP. These MOUs include provisions emphasizing that the FBI IP enrollments and searches will be limited to authorized agencies for authorized purposes and that all CJIS policies regarding access to and use of CJIS information apply. All authorized NGI users interfacing with the FBI IP are required to adhere to these CJIS policies.

Section 534 of Title 28 United States Code, permits the FBI to cancel the dissemination of information under its authority if it is disclosed outside the receiving agency or related agencies. 28 CFR § 20.33 provides supplemental guidance regarding the dissemination of criminal history record information, including identification of authorized recipients and potential sanctions for unauthorized disclosures. These regulatory privacy protections supplement the privacy provisions of the Privacy Act of 1974. The FBI also maintains pursuant to other standards and regulations, long-standing and extensive system security standards and operating policies applicable to all system users. Authorized users must comply with applicable security and privacy protocols addressed in the CJIS Security Policy. Federal and state audits are performed to ensure compliance. The CSO is responsible for implementing and ensuring compliance with the CJIS Security Policy.

The main method for the transmission of biometric submissions is electronically, via the CJIS WAN, a telecommunications infrastructure that connects authorized agencies to the CJIS host computer systems. The purpose of the CJIS WAN is to provide a secure transport mechanism for CJIS 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 and authorized non-law enforcement agencies in all fifty states. Agencies transmit and, in turn, CJIS responds via the CJIS WAN. The CJIS WAN transmission hardware is configured by FBI personnel, transmission data to and from CJIS is encrypted, and firewalls are mandated and in place. Electronically, the iris images are supported through the EBTS, which currently supports fingerprint, palm print, latent submissions, face photos, and iris images. The EBTS provides proper methods for external users to communicate with the CJIS systems for the transmission of biographic and biometric information for purposes of criminal or civil identification.

CJIS 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 thereafter.

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 particular 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. The audits assess and evaluate users' compliance with CJIS technical security policies, regulations, and laws applicable to the criminal identification and criminal history information (CHRI), and terms of the applicable user agreements or contracts. Deficiencies identified during audits are reported to the CJIS APB and Compact Council Sanctions Committees. Access may be terminated for improper access, use, or dissemination of system records. In addition, each 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 employees 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.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7. Further notice will be provided by this PIA.	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

	Yes, individuals have the opportunity to decline to provide information.	Specify how:
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: Iris images are collected pursuant to the criminal justice processing of an individual, such as an arrest or an incarceration..

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Iris images are collected pursuant to the criminal justice processing of an individual, such as an arrest or incarceration.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

Because the iris images and associated information in the FBI IP are collected in connection with law enforcement investigations and prosecutions, individuals generally do not have the right or opportunity to object to the collection of this information or the retention and searching of this information in the FBI IP. The privacy risks associated with lack of notice to affected individuals about the collection, maintenance, and use of iris images are mitigated by the general notice to the public via

the NGI System of Notice (SORN) published in the Federal Register and the publication of this PIA. Also, information in the FBI IP is collected during criminal justice processing of the individual of which the individual should be specifically aware. Similarly, the iris images submitted for search will be taken incident to direct involvement with a criminal justice agency of which the individual should be specifically aware.

Section 6: Information Security

6.1 Indicate all that apply.

X	A security risk assessment has been conducted. A security risk assessment for NGI, which included the planned iris repository, was completed in August 2013.	
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: Controls are documented in the NGI Security Requirements Traceability Matrix (SRTM).	
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: Full testing for NGI was conducted in August 2013. The system, including the iris repository which is within its security accreditation boundary, is further evaluated quarterly to ensure safeguards remain in place	
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: NGI: 04/30/2014, which expires on 04/29/2017. The iris repository received authority to operate in 04/2015 and is a major application within the NGI accreditation boundary.	
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: As NGI is the replacement system for IAFIS, auditing for NGI is being conducted in the same manner as it was for IAFIS.	
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.	
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.	
X	The following training is required for authorized users to access or receive information in the system:	
	X	General information security training
	X	Training specific to the system for authorized users within the Department.
	X	Training specific to the system for authorized users outside of the component.
		Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure. [In answering the question, you should discuss user

authentication, data encryption, and NIST Confidentiality Safeguard Controls.]

Please see Section 4.2 for specific access and security control descriptions. In addition, the NGI system NIST 800-53 security control baseline is at the HIGH impact level of assurance. Security controls are continually assessed during the development life cycle for compliance and to ensure appropriate mitigation strategies have been implemented commensurate with the HIGH impact level of assurance.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. In May 2016, a new/updated system of records notice for this system of records was published. See Next Generation Identification System, 81 Fed. Reg. 27,284 (proposed May 5, 2016). The most recent complete notice is the Fingerprint Identification Records System (FIRS) (Justice/FBI-009) (64 Federal Register (FR) 52343, 52347 (09/28/1999); 66 FR 33558 (06/22/2001); 70 FR 7513, 7517 (02/14/2005); 72 FR 3410 (01/25/2007).
	Yes, and a system of records notice is in development. .
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

All information in the FBI IP is retrieved by iris images or other biometric or descriptive identifiers, as explained above in Section 1 of this PIA. Information about individuals, regardless of citizenship, is retrieved by searching on these identifiers.