Federal Bureau of Investigation

Privacy Impact Assessment
for the
Next Generation Identification (NGI)
Rap Back Service

Issued by:

Ernest J. Babcock
Senior Component Official for Privacy
FBI

Approved by: Erika Brown Lee, Chief Privacy and Civil Liberties Officer,
U.S. Department of Justice

Date approved: December 15, 2016

Section 1: Description of the Information System

Introduction

The Criminal Justice Information Services (CJIS) Division has provided state-of-the-art fingerprint identification and criminal history services through its Integrated Automated Fingerprint Identification System (IAFIS) for many years.[1] CJIS has replaced the IAFIS fingerprint services and provided new and advanced services for other biometrics with the incremental implementation of the Next Generation Identification (NGI). This Privacy Impact Assessment (PIA) addresses NGI's Rap Back Service, which is one of the services delivered as part of NGI's final increment. In a previous PIA, CJIS provided notice of the retention and searching of noncriminal justice (hereinafter "civil") fingerprints in NGI that are received in accordance with federal authority (e.g. federal statute, Presidential Executive Order) or state authority (e.g., state statutes pursuant to Public Law 92-544).[2] For many decades, federal and state agencies and other authorized entities have collected and submitted civil fingerprints to the FBI for criminal background checks for noncriminal justice purposes. Due to capacity limitations, IAFIS did not retain most of the civil fingerprints submitted; once processed, the fingerprints were destroyed. NGI, however, will now retain all civil fingerprints as authorized by the submitting agencies. This retention of civil fingerprints provides the foundation for the Rap Back Service.

Non-Criminal Justice Rap Back

Currently, authorized agencies submit the civil fingerprints of employment applicants, licensees, and other individuals in positions of public trust on a periodic basis to determine if the individuals have engaged in criminal conduct that would prohibit the holding of such positions or licenses. Some examples of these positions or licenses would be in the education, financial, security, and healthcare professions. With implementation of NGI, the authorized agencies may choose to submit the civil fingerprints for retention and subscription into the Rap Back Service. This will result in an ongoing review or continuous evaluation of the criminal history status of each individual as long as the individual remains in a position of trust. In other words, rather than authorized agencies resubmitting civil fingerprints for periodic background checks, the civil fingerprints will be retained and searched for as long as the individuals are appropriately subscribed to the Rap Back Service. The technology used by the Rap Back Service provides for a continuous vetting of the person's suitability for his/her position of trust by providing timely notification to the authorized agency should the individual be arrested or if there is other subsequent criminal activity associated with that identity record in NGI, such as warrant or sex offender updates. Other relevant updates, such as expungements

[1] See https://www fbi.gov/services/records-management/foipa/privacy-impact-assessments for links to various privacy impact assessments involving IAFIS.

[2] For additional information, see the "NGI Retention and Searching of Non-Criminal Justice Fingerprint Submissions" Privacy Impact Assessment issued in February 2015 at https://www fbi.gov/services/records-management/foipa/privacy-impact-assessments/next-generation-identification-ngi-retention-and-searching-of-noncriminal-justice-fingerprint-submissions.

or death notices, may also be provided to the authorized agency.

Utilizing the Rap Back Service begins with a criminal history background check for an initial determination of suitability for a position of trust. Following a favorable determination from the initial background check, a subscription to the individual in NGI may be created. Noncriminal justice Rap Back subscriptions may only be established by a government agency or a non-governmental entity that has been authorized by federal statute, federal executive order, or state statute approved by the United States Attorney General, to receive Criminal History Record Information (CHRI) for noncriminal justice purposes and assigned an originating agency identifier (ORI) by the FBI CJIS Division.[3]

The decision to subscribe the individual may occur simultaneously with the initial background check or in a subsequent transaction. Upon subscription, the individual's fingerprints will be continuously searched against the criminal, civil, and latent fingerprints retained in NGI. All established Rap Back subscriptions will include notification of any subsequent arrest as a "triggering" event. Additional triggering events may be selected by the authorized agency and could include: criminal dispositions, expungements, warrants, sex offender entries, and death notifications. Certain federal agencies, in very limited circumstances, may also receive civil information as triggering events if within their legal authorities.[4] It is important to note that if a current fingerprint submission appears to match existing latent fingerprints on file, only the submitter of the latent fingerprints will be notified.

To assist with keeping data related to the Rap Back Service accurate and up-to-date, all subscriptions are required to have an expiration/validation date as part of Rap Back's privacy risk mitigation strategies. Validation requires the subscriber to periodically affirm that its subscriptions are still valid, and mandatory expiration dates have been established to ensure that NGI Rap Back validation takes place regularly. As explained in more detail below, in some cases, a one-year validation cycle will be entered into NGI's Rap Back Service with a one-year expiration date. In other instances, the expiration/validation date will be the expiration of a professional license or other authorized term. In other instances, the expiration/validation date will be the maximum authorized term of five years. Whatever the expiration date that is established, however, the authorized agency must verify at that time that it remains authorized to receive the triggering event information regarding the individual, and if the agency fails to verify continued authorization, the subscription will be cancelled.

To ensure that individual privacy rights are not compromised by a Rap Back subscription and to maintain the integrity of the NGI's Rap Back data and service, each Rap Back subscription must incorporate one of five privacy risk mitigation strategies. These five privacy risk mitigation strategies, approved by the National Crime Prevention and Privacy Compact Council (Compact Council)[5], were

[3] An ORI is a unique number that is assigned to each agency authorized to access NGI for authorized purposes. *See also* Section 4.2 of this PIA.

[4] For the vast majority of authorized agencies, there is no legal authority to receive civil information; however, for Intelligence Community agencies that have employees with security clearances in rap back, they may receive limited civil information, such as an employee applying for additional employment elsewhere.

[5] The Compact Council was created pursuant to the National Crime Prevention and Privacy Compact Act of 1998, Title 42

established utilizing specific tools, including training, auditing, and validation. An authorized agency may choose:

(1) *Pre-Notification with Validation or Mandatory Expiration within Five Years.* With pre-notification, the submitting agency receives only an initial notification that an event related to the subscribed individual has occurred. This ensures that an individual's information is not provided to an agency that no longer has authority to receive such information. Pre-notification requires the subscriber to verify its current authority to receive the CHRI or other Rap Back information related to that specific individual. In other words, the subscriber must confirm that the individual remains in the relevant position of trust for which the subscription was entered before receiving the triggering event information. Validation and expiration dates ensure that Rap Back subscriptions in NGI remain current and accurate even if they are never accessed during the course of the Rap Back subscription. If pre-notification is used, the subscriber is not required to validate before the 5 year maximum term.

(2) *Authority for the Duration of License.* Applicable laws or regulations may assign a certain time limit for the duration of a license, such as a nursing license. In those instances, the expiration of the Rap Back subscription may be set for more than five years if permitted by the professional license, but the validation date must remain within five years for the subscription to stay active;

(3) *Statutory or Regulatory Authority for Set Term.* Likewise, applicable laws or regulations may provide authority for set terms, such as the duration of a security clearance. In those instances, the expiration of the Rap Back subscription may be set for more than five years if permitted by the relevant legal authority, but the validation date must be within five years for the subscription to stay active;

(4) *One-Year Validation or Expiration.* For any subscription, a one-year validation or one-year mandatory expiration date is sufficient and may serve in lieu of pre-notification. In other words, due to the frequency of review of the agency's Rap Back subscriptions, the subscriber may receive the CHRI or other Rap Back information when a triggering event occurs; or

(5) *Subscription Synchronization through Automated or Formalized Procedures.* Rather than validation or expiration at certain points in time, subscribing agencies maintain synchronized records with NGI on an ongoing basis to ensure current and accurate Rap Back subscriptions. Formal validation is still conducted at a minimum of every five years to ensure Rap Back subscriptions accurately reflect the current status of the individual.

Criminal Justice Rap Back

NGI's Rap Back Service will also provide timely notifications to authorized criminal justice agencies regarding individuals under the supervision of a criminal justice agency or under authorized law enforcement investigation. Criminal justice Rap Back subscriptions may not be established for an individual whose fingerprints are only in NGI for civil purposes. At least one fingerprint-based criminal event must exist before a criminal justice subscription will be permitted.

U.S.C. Chapter 140. It was established to facilitate the exchange of authorized interstate criminal history records for non-criminal justice purposes.

The two types of criminal justice Rap Back are 1) supervisory and 2) investigatory. Supervisory Rap Back is used by law enforcement agencies, probation and parole officers, and other criminal justice entities to be advised of subsequent criminal activity of persons under their supervision, such as probationers, parolees, sex offenders, persons under direct court supervision, and other officially supervised persons. Investigatory Rap Back is used by law enforcement agents to be advised of criminal activities of persons under investigation.

Utilizing the Rap Back Service for criminal justice purposes begins with subscription to an individual's criminal fingerprints. For supervisory rap back, the fingerprints of a probationer, parolee, or convicted sex offender will already be maintained in NGI. To receive notification of subsequent activity, the authorized agency simply subscribes to the fingerprints in NGI. For investigatory rap back, the law enforcement agency must subscribe to an existing set of criminal fingerprints maintained in NGI or may add criminal fingerprints at the time of the rap back subscription. An investigatory rap back subscription may not be placed on an individual with only civil fingerprints in NGI.

Criminal justice Rap Back subscriptions may only be established by recognized criminal justice agencies who have been assigned criminal justice ORIs by the FBI CJIS Division. As such, criminal justice agencies may not establish a Rap Back subscription for an individual unless they are authorized under current policy to perform a criminal history query on the individual at the time the subscription is established and for the duration of the supervision or investigation. The criminal justice agency must be already authorized to access the individual's criminal history in order to automate the process with the Rap Back Service. Criminal justice subscriptions may only be established for cases that have been assigned an official agency case number and for which the statute of limitations has not run. All criminal justice Rap Back subscriptions must include the subscriber's case number in the originating case number (OCA) field; otherwise, the subscription will be rejected. The purpose of the OCA requirement is to provide an additional data element to CJIS that the criminal justice subscription is supported by an official, open law enforcement investigation.

Like non-criminal justice Rap Back, all established criminal justice Rap Back subscriptions will include notification of any subsequent arrest event as a "triggering" event and additional triggering events (e.g., warrants, deaths, expungements) may be selected by the subscriber. These triggering events will not include civil events such as fingerprints submitted for licensing or employment purposes. By default, all criminal justice Rap Back subscriptions have a mandatory expiration date. For supervisory subscriptions, the maximum subscription term is five years. For investigatory subscriptions, the maximum subscription term is one year, with the agencies being advised to ensure Rap Back subscriptions are set to the shortest appropriate date so that no subscription is maintained without justification. Although renewal of these subscription terms may be possible, these maximum terms were determined by the FBI, in consultation with state and local law enforcement partners, to be an adequate length of time for supervisory and investigatory rap back subscriptions.

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		x	Financial account		
Taxpayer ID			Driver's license		x	Financial transaction		
Employee ID		x	Passport		x	Patient ID		
File/case ID		x	Credit card					
Other identifying numbers (specify): Most identifying numbers are optional but may be associated with fingerprints by the submitting agencies.								

General personal data								
Name		x	Date of birth		x	Religion		
Maiden name		x	Place of birth		x	Financial info		
Alias		x	Home address		x	Medical information		
Gender		x	Telephone number			Military service	x	
Age		x	Email address			Physical characteristics	x	
Race/ethnicity		x				Mother's maiden name		
Other general personal data (specify): The Rap Back service operates within the NGI system, which as has been noted, holds a variety of personal data elements. However, the Rap Back service searches only the fingerprints in NGI and then notifies subscribers about any fingerprint matches.								

Work-related data								
Occupation		x	Telephone number			Salary		
Job title		x	Email address			Work history		
Work address		x	Business associates					
Other work-related data (specify): Work-related data may be provided by the submitting agencies, but the data is not required and is not searchable within NGI.								

Distinguishing features/Biometrics								
Fingerprints		x	Photos		x	DNA profiles		
Palm prints		x	Scars, marks, tattoos		x	Retina/iris scans		
Voice recording/signatures			Vascular scan			Dental profile		

Distinguishing features/Biometrics
Other distinguishing features/biometrics (specify): The Rap Back Service requires the submission of fingerprints and all enrollment, searching, and dissemination is based on fingerprint-based identification. As noted above, other personal information and biometrics also may be associated with fingerprints by the submitting agencies, but this is not searched by Rap Back.

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)
n/a

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 fingerprints and associated information required for enrollment in the Rap Back Service will not be obtained directly from the individual; rather, authorized criminal justice and noncriminal justice agencies will submit the fingerprints.					

Government sources					
Within the Component	x	Other DOJ components	x	Other federal entities	x
State, local, tribal	x	Foreign			
Other (specify):					

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.)

As discussed in Section 1, participation in NGI's Rap Back Service for non-criminal justice purposes requires the retention of civil fingerprints submitted for criminal history background checks. The fingerprints enrolled in the Rap Back Service are continuously searched by and against criminal (including latent) and non-criminal justice fingerprints subsequently submitted to NGI. To address the risk that civil applicants and licensees may be unaware of the enhanced retention and searching of their fingerprints, they are provided a Privacy Act Statement on both the hard-copy cards and the electronic live scan devices used for fingerprint collection. The Privacy Act Statement advises all applicants and licensees of the authorities for the collection of their fingerprints, how their fingerprints will be retained and searched in NGI, and how their information will be shared. Since the Rap Back Service creates no new authority for the submission of civil fingerprints, each submitting agency must rely on its existing legal authority or obtain legal authority to submit, retain, and search fingerprints in NGI; these authorities also serve to provide notice to the civil applicants and licensees. Finally, this PIA, the NGI system of records notice, and other official FBI public communications provide notice of the Rap Back Service.

Participation in NGI's Rap Back Service for non-criminal justice purposes also creates risks that triggering event information and/or personally identifiable information will be disseminated to unauthorized recipients or that subscriptions could remain in NGI when the agency no longer has an official interest in the individual. For example, if an individual is no longer employed in the relevant position of public trust, the submitting agency may no longer have the authority to receive information regarding that former employee. To mitigate these risks, each Rap Back subscription must incorporate one of the five privacy risk mitigation strategies (listed in Section 1) to ensure continued authorization to receive Rap Back information. These strategies rely on a combination of pre-notification, validation, and expiration dates. In the case of pre-notification, the submitting agency receives only an initial notification that an event related to the subscribed individual has occurred. The submitting agency must then confirm the accuracy and currency of that subscription in order to receive the triggering event information. Validation and expiration dates ensure the non-criminal justice Rap Back subscriptions in NGI never become stale even if those records are never accessed due to triggering events. Should an individual retire or leave employment for any reason, the relevant subscription will be reviewed and removed from the Rap Back Service in a timely manner. The maximum period of time a non-criminal justice Rap Back subscription can remain in NGI without validation by the submitting agency is five years. At that time, the submitting agency must confirm that the subscription should remain in the Rap Back Service or it will be removed.

Participation in NGI's non-criminal justice Rap Back Service also creates various risks such as unauthorized subscriptions, improper access to data, or other misuse of data. These risks are mitigated in many ways. Before a civil agency may submit subscriptions for the Rap Back Service, it works with the CJIS Division to complete an agreement that includes best practices for policy, technology, privacy, and other requirements for managing subscriptions. The completion of the agreement gives the CJIS Division an opportunity to make sure the submitting agency fully understands the Rap Back Services and is employing the necessary processes to assist with mitigating risks. Criminal justice agencies are already trained on the controls in place with respect to the appropriate use of CHRI obtained from CJIS. In addition, training and auditing continue to be integral components to protect against improper access to or use of the data. In an effort to ensure all legislative and agency policy protections are being implemented, CJIS has an established Audit Unit that regularly visits entities that are authorized to collect and submit fingerprints. 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 wrongfully accessed or disseminated, both the CJIS Advisory Policy Board (APB) and the Compact Council have established sanction committees to address the possible misuse. Finally, the system will store information regarding the dissemination of information and related data in audit logs. Dissemination of information will be linked to the authorized user and the agency that requested the information.

Additionally, as discussed above in Section 1, both non-criminal justice and criminal justice Rap Back subscriptions may only be established by agencies or entities that have been assigned an ORI by CJIS. Therefore, with regard to non-criminal justice subscriptions, only government agencies or non-governmental entities that have been authorized by federal statute, federal executive order, or state statute will have access to Rap Back information. With respect to investigative subscriptions, only law enforcement agencies that would be authorized to conduct criminal inquiries of the NGI system will be permitted to access Rap Back information. The NGI Rap Back Service does not change any controls or any rules for the use of CHRI. Moreover, criminal justice Rap Back subscriptions may not be placed on an individual whose fingerprints are only in NGI for civil purposes; at least one fingerprint-based criminal event must exist before a criminal justice subscription may be permitted. Criminal justice subscriptions may only be established on identities associated with an open law enforcement investigation and must provide the specific case number. Likewise, as discussed above in Section 1, all criminal justice Rap Back subscriptions will, by default, have a mandatory expiration date. However, agencies are encouraged to set their criminal justice Rap Back subscriptions for the shortest time period possible. For supervisory subscriptions (e.g. probation and parole), the maximum subscription term is five years. For investigative subscriptions, the maximum subscription term is one year, with the caveat that the subscription should be set to the shortest appropriate date so that no subscriptions are maintained without justification.

Another privacy risk could be maintenance of erroneous data within NGI's Rap Back Service. The privacy risk of maintaining erroneous data is lessened because the FBI and its partners have a substantial interest in ensuring the accuracy of information in the NGI system and in correcting any erroneous information of which they may become aware. Additionally, this risk is further lessened 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. The FBI has a vigorous compliance and audit system to ensure that it faithfully adheres to these legal obligations. Finally, this risk is further lessened to the extent that an agency that contributes information to NGI has a process in place for access to or correction of its source records.

The retention of additional data which support NGI's Rap Back Service also presents a correspondingly increased risk that the FBI will be maintaining more information that is subject to loss or unauthorized use. Notably, the existing IAFIS system security requirements and user rules regarding access and dissemination of criminal history information remain unchanged with the implementation of NGI.[6] The risk of loss/unauthorized use is mitigated by the strong system, user, site, and technical security features present in NGI which are described in later sections of this PIA.

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
	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): non-criminal justice background checks for purposes such as employment, licensing, and security clearances		

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 below, the FBI has statutory authority to collect, preserve, and exchange biographic and biometric information for criminal, civil, and national security purposes. In line with that authority, part of the CJIS Division's mission is to reduce terrorist and criminal activities by improving and expanding biometric identification and criminal history information services. NGI enhancements will

[6] See Note _7__infra.

allow CJIS to continue to provide criminal justice, national security, and authorized civil agencies with timely identification services relevant to their missions. In addition, part of NGI's mission is also to ensure that persons serving in positions of public trust continuously meet the requirements to be chosen for, and to remain in, those positions. Although civil fingerprints have been collected by the FBI for several decades, the mandate for the FBI to retain civil fingerprints has become broader in recent years. For example, there is legal authority that requires fingerprint-based background checks of applicants for an expanded number of employment positions and the Security Clearance Information Act permits certain federal agencies to conduct fingerprint-based background checks to assist with determining eligibility for access to classified information and national security duties. Likewise, other federal legislation, such as the National Child Protection Act, provides state and local governments with the authority to conduct fingerprint-based background checks for those who work with vulnerable populations, such as children, the elderly, and the disabled.

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 USC §§533, 534; 42 USC §3771; USA PATRIOT ACT; Public Law 92-544; Security Clearance Information Act; National Child Protection Act; Volunteers for Children Act; Adam Walsh Child Protection and Safety Act; Serve America Act
x	Executive Order	E.O. 8781, 8914, 10450, 13311, 13356
x	Federal Regulation	28 CFR 0.85, 20.31, 20.33, 50.12
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	(This list is composed of significant examples of background check authority and is not comprehensive)

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.)

NGI data will be retained in accordance with the applicable retention schedules approved by the National Archives and Records Administration (NARA). NARA has approved the destruction of

fingerprint cards and corresponding indices 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 record information and NGI transaction logs are to be permanently retained. Biometrics and associated biographic information may be removed from the NGI system earlier than the standard NARA retention period pursuant to a request by the submitting agency or the order of a court of competent jurisdiction. For the first part of the question, see the "NGI Retention and Searching of Non-Criminal Justice Fingerprint Submissions" Privacy Impact Assessment issued in February 2015.

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.)

The privacy risks from the use of the information are described in Section 2.3. The initiative described in this PIA will be subject to the same extensive security protections, access limitations, and quality control standards already in existence for IAFIS and further augmented by 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 or agency's search and retrieval of the biometric data. The CJIS Audit Unit conducts internal and external on-site audits of user agencies to assess and evaluate compliance with the CJIS Security Policy[7] 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. When rap back subscriptions are cancelled or expire, fingerprints that were the basis for Rap Back searches under that subscription are maintained in NGI unless an independent removal process is initiated. For example, fingerprints will be purged from the system when requested by the submitting agency or as a result of a court order, such as an expungement.

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.

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

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

The privacy risks associated with the NGI Rap Back Service regarding disclosure or sharing of information and how those have been mitigated are described in Section 2.3.

In addition, NGI information (in the context of which the Rap Back service runs its checks) is available to Department of Justice (DOJ) components when there is a need for the information to perform official duties, pursuant to 28 U.S.C. § 534 and 5 U.S.C.§ 552a(b)(1). Information is disclosed only to DOJ users who have been authorized access to the information in the NGI system. The FBI shares information with the National Security and Criminal Divisions of DOJ, as well as internal DOJ components such as the United States Marshals Service, the Drug Enforcement Administration, the Bureau of Prisons, and the Bureau of Alcohol, Tobacco, Firearms, and Explosives.

Biographic and biometric data within NGI will also be shared with local, state, federal, tribal, foreign, international, and joint agencies as permitted by Federal and State statutes, Federal and State executive orders, or regulation or order by the Attorney General. Information is shared with authorized noncriminal justice agencies and other regulatory entities for employment suitability checks, permits, identity verification, and licensing in accordance with applicable laws, regulations and policies. NGI

will maintain data provided only by authorized agencies, which are responsible for ensuring that accurate and complete biographic and biometric information is submitted in the first instance, in accordance with CJIS data quality standards and operating policies.

Privacy protection is provided by 28 U.S.C. § 534 which provides that the dissemination of information under its authority is subject to cancellation if shared information 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 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. Federal and State audits are performed to ensure compliance. The CJIS System Officer (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 Wide Area Network (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, biometrics will be supported through the Electronic Biometric Transmission Specification (EBTS)[8], which currently supports fingerprint, palm print, latent fingerprint, and photo submissions. 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 retested thereafter. Access to NGI will be by the same users who currently have access to IAFIS; this initiative does not change the procedures that are used to determine which users may access the system.

Authorized users will have the ability to directly enroll biometrics into or delete biometrics from existing files within NGI based on their roles. The systems are not available to users unless there has been an application for, and assignment of, an ORI (defined earlier) unique to each using entity. Each

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

user may only access the 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 dissemination of identification records to the applicable ORI. Full access ORIs are provided to criminal justice agencies and other agencies as directed by Federal legislation for criminal justice purposes. Limited access ORIs are provided to noncriminal justice agencies requiring access to FBI-maintained records for official and authorized purposes. Most noncriminal justice agencies and entities have been assigned limited access ORIs and are entitled to criminal history information after first submitting fingerprints and identifying the authority for such submissions. The FBI sends notifications electronically. Each state may send notifications to their respective agencies in different formats.

Like IAFIS, the NGI System Design Document includes requirements to maintain chronological transaction audit logs for authorized purposes. All users are subject to periodic on-site audits conducted by both a user's own oversight entity and the CJIS 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, and terms of the applicable user agreements or contracts. Deficiencies identified during audits are reported to the CJIS Division 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.

Internal users of the system are FBI employees and contractor personnel who must complete annual information security and privacy 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.	
x	Yes, notice is provided by other means.	Specify how: [Civil applicants will be provided with notice via fingerprint cards, live-scan fingerprint devices, and/or other publications.]
[ ]	No, notice is not provided.	Specify why not: [ ]

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

x	Yes, individuals have the opportunity to decline to provide information.	Specify how: [Civil applicants may decline to submit fingerprints; however, a fingerprint-based background check is often a prerequisite for employment and licensing.]
x	No, individuals do not have the opportunity to decline to provide information.	Specify why not: [Criminal justice Rap Back subjects are under lawful criminal supervision or investigation.]

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

[x]	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how: [Civil applicants consent to the retention and searching of their fingerprints when they apply for employment, licensing, or other benefit.]
x	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: [Criminal justice Rap Back subjects are under lawful criminal supervision or investigation.]

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.

[The privacy risks associated with lack of notice to affected individuals about the collection, maintenance, and use of additional fingerprints are mitigated by the general notice to the public via the System of Records Notice (SORN) published in the Federal Register and the NGI PIAs available on www.fbi.gov.

For civil applicants, specific notice is typically the responsibility of the agency collecting the fingerprints. Civil information is often collected on the FBI Applicant Fingerprint Card (FD-258) or an

equivalent paper or electronic consent form. It is anticipated that most civil fingerprints will be collected via live scan devices in the near future. The Privacy Act Statement on the FD-258 fully advises the applicant of the retention and use of civil fingerprints in NGI. Civil applicants may be legislatively required to submit fingerprints as a condition for employment, licensing, security clearances, positions of public trust, and volunteer positions. Inasmuch as the choice to apply for employment and licensing is voluntary, the individual may choose not to apply for positions that require the submission of fingerprints. Declining to submit fingerprints, however, may have an adverse impact with respect to the benefit requested, depending upon the governing laws and policies pursuant to which the FBI background check was initiated.

For criminal justice Rap Back subscriptions, the opportunity for individuals to decline to provide information or to consent to uses of their information is not practicable. A person under arrest generally has no opportunity or right to refuse the collection of fingerprints. Nevertheless, any use of the information must comply with the provisions of any applicable law, including the Privacy Act.

Title 28 C.F.R. part 16, subpart A, provides general guidance on access to information in FBI files pursuant to the Freedom of Information Act, and 28 C.F.R. part 16, subpart D, provides general guidance regarding access to, and amendment of, information in FBI files pursuant to the Privacy Act. However, certain NGI records are exempt from access and amendment under the Privacy Act. (See 28 C.F.R. § 16.96 (e) and (f)). Title 28 C.F.R. §§ 16.30-16.34 and § 20.34 establish alternative procedures for a subject of an FBI criminal identification record (i.e. rap sheet) to obtain a copy of his record for review and correction. If, after reviewing his identification record, the individual believes that it is incorrect or incomplete in any respect and wishes changes, corrections, or updating, he may make application directly to the agency that contributed the questioned information. The individual may also direct his challenge to the FBI CJIS Division. The FBI will then forward the challenge to the agency that submitted the data requesting that agency to verify or correct the challenged entry.

The opportunity to seek access to or redress information in the source records of a contributing local, state, federal, or tribal agency will be controlled by the laws and procedures applicable to that agency. To the extent that such an agency has a process in place for access to or correction of the contributing agency's source records, individuals may avail themselves of that process. If the process results in a correction of the source records, the contributing agency should, in turn, make appropriate corrections in the information contributed to NGI.

Officials making the determination of suitability for licensing or employment must provide the applicants the opportunity to challenge the accuracy of information contained in the FBI identification record. These officials must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in Title 28 CFR § 16.34. Officials making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record (see 28 CFR §50.12).

Section 6: Information Security

6.1 Indicate all that apply.

x	A security risk assessment has been conducted. A full risk assessment was conducted in January 2014.	
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 was conducted in January of 2014. The system 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: April 30, 2014.	
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 conducted—as was auditing for IAFIS—subject to the CJIS Security Policy.	
x	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act. Contractors provide a variety of general support and development services for NGI and in some cases may have access to system data. The extent of access will vary based on the nature of the contract requirements and will be subject to appropriate non-disclosure and use limitations. Existing contracts contain appropriate security requirements and are subject to extensive privacy protections built into the existing infrastructure and policies, such as limited access, secure location, audits, and Privacy Act clauses provided by the Federal Acquisition Regulation.	
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.

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 or has already been 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 for reasons unrelated to the introduction of the information technology at issue here. *See* Next Generation Identification System, 81 Fed. Reg. 27,284 (proposed May 5, 2016). Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: "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 NGI is retrieved by the Rap Back service by fingerprints 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.