

Federal Bureau of Investigation



Privacy Impact Assessment for the [Next Generation Identification Rap Back Service]

Issued by:
Erin M. Prest, Privacy and Civil Liberties Officer

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

Date approved: June 13, 2025

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

This Privacy Impact Assessment (PIA) is an update to the Next Generation Identification (NGI) Rap Back Service PIA published in December 2016. Specifically, this PIA addresses the implementation and expansion of the Rap Back Service since its initial deployment. The Rap Back Service is managed by the FBI's Criminal Justice Information Services (CJIS) Division and operates within the NGI System, the FBI's national biometric and criminal history repository.

The Rap Back Service provides automated, accurate, and timely responses to authorized agencies that submit noncriminal justice (hereinafter "civil") fingerprints for searching and retention in the NGI System. Federal, state, and other authorized entities submit civil fingerprints to the FBI for criminal background checks of applicants seeking employment, licenses, security clearances, positions of public trust, and government benefits. The Rap Back Service permits these civil fingerprints to be retained in the NGI System and continuously searched rather than requiring periodic re-submission of the fingerprints for background check purposes, providing convenience for the individuals undergoing background checks and potential benefits for the public. Likewise, the Rap Back Service is made available to criminal justice agencies for retention and continual searching of fingerprints for subjects of supervised release or active criminal investigations.

Section 2: Purpose and Use of the Information Technology

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

Noncriminal Justice Rap Back

For decades, federal, state, and other authorized entities have collected and submitted fingerprints to the FBI for criminal background checks for noncriminal justice purposes. The purposes for which such "civil fingerprints" are submitted may include employment, licensing, and the receipt of governmental benefits. Entities receiving the results of these criminal background checks for non-criminal purposes must be authorized by federal statute, federal executive order, or state statute, or approved by the Attorney General to receive criminal history record information (CHRI) for noncriminal justice purposes. The civil fingerprints are retained by the FBI pursuant to its statutory authority to collect, preserve, and exchange biographic and biometric identity information for criminal, civil, and national security purposes.

The legal uses and mandates for the FBI to collect and retain civil fingerprints have become more extensive in recent years. For example, certain federal agencies are required to conduct fingerprint-

based background checks to assist with determining eligibility for access to classified information and the performance of national security duties. Additionally, many federal executive agencies have been mandated to participate in the continuous vetting of their workforces, and the Rap Back Service provides CHRI when required as part of such continuous vetting requirements.¹ Other federal statutes permit CHRI to be shared with state and local governments with the authority to conduct fingerprint-based background checks of those who work with vulnerable populations such as minors, the elderly, and disabled individuals. Currently there are eleven state agencies, eleven federal agencies, and ten other authorized entities approved to participate in the NGI Noncriminal Justice Rap Back Service. The CJIS Division continues to engage with prospective agencies and expects more state, federal, tribal and territorial participants in the future.

In general, Public Law 92-544, codified at Title 34 United States Code Section 41101, permits the FBI to exchange CHRI with officials of state and local governments if the state employment and licensing statutes meet certain criteria and are approved by the Attorney General, whose approval authority has been delegated to the FBI.² This statute authorizes thousands of civil fingerprint-based background checks each year for many important professional fields, such as education, medical, and financial services.

To participate in the Noncriminal Justice Rap Back Service, the prospective agency must have legal authority to submit and retain fingerprints in the NGI System and allow the fingerprints to be continually searched by subsequent fingerprint submissions to the system. Authorized agencies no longer need to submit the civil fingerprints of applicants, licensees, and other individuals in positions of public trust, on a periodic basis to determine if individuals have engaged in criminal conduct. Rather, the authorized agencies may choose to submit the civil fingerprints for retention in the NGI System and create a subscription in the Noncriminal Justice Rap Back Service. This subscription results in an ongoing review or continuous vetting of the CHRI for each enrolled individual.

When an individual is fingerprinted for a specific position or benefit, an approved entity will fingerprint the individual, collect associated biographic information, and electronically submit the information to the NGI System to be searched and retained. The decision to subscribe the individual in the Rap Back Service may occur simultaneously with the initial fingerprint submission or in a subsequent Rap Back Service transaction. The Rap Back subscription is established through optional Rap Back request fields in the electronic fingerprint submission. Placing a value in the Rap Back category field indicates to the NGI System that the civil fingerprint submission is also a Rap Back subscription request. If a Rap Back subscription is requested for a fingerprint submission, the agency must also request retention of the fingerprints or the subscription will be rejected. If an agency chooses to subscribe an individual in the Rap Back Service after the initial criminal background check, it must provide additional biographic information, the Universal Control Number (UCN), a number assigned to each person with an identity within the NGI System, and either a new set of fingerprints or a civil event identifier number that links the previously submitted civil fingerprints to the individual with that identity.

¹ See Executive Order 13467 Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information- June30, 2008; Federal Investigative Standards, revised 12/2012.

² See <https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/public-law-92-544>

Upon subscription, the individual's fingerprints will be continually searched against criminal, civil, and latent fingerprints within the NGI System. Once the Rap Back Service subscription is set, the NGI System will return information to authorized agencies based only on an identification determined by tenprint fingerprints or the UCN. Authorized agencies will receive electronic notification of any arrest of the individual. Authorized agencies are also notified of any identity maintenance which may occur including identity deletion, restoration, and/or consolidation. In addition to arrest and identity maintenance notifications, the Rap Back Service provides notice of other "triggering" events chosen by the authorized agency. These events include dispositions (i.e., information disclosing that criminal proceedings have been concluded and the nature of the termination),³ the addition/deletion of wants (that is, individuals who are wanted), and warrants, the addition/deletion of sex offender registry entries, and death notifications. If the individual's fingerprints appear to match latent fingerprints in the NGI System's Unsolved Latent File⁴, only the submitter of the latent fingerprints will be notified.

The NGI Noncriminal Justice Rap Back Policy and Implementation Guide (Rap Back Guide) provides the policy, legal, privacy, and security requirements for agencies that participate in the Noncriminal Justice Rap Back Service. It is important to note that the Rap Back Guide is specific to the additional requirements of the Rap Back Service; these authorized agencies have pre-existing User Agreements and Memoranda of Understanding with the CJIS Division to manage the submission of civil fingerprints, including the legal, technical, and security requirements. The Rap Back Guide applies to both subscribers and submitters utilizing the Rap Back Service. A subscriber, also known as an authorized recipient, refers to the agencies described above which are authorized under statute, executive order, or regulation to receive CHRI of identities enrolled in the Rap Back Service. A subscriber often uses the services of a submitter, which is a State Identification Bureau (SIB)⁵, authorized federal agency, or authorized contractor that submits the civil fingerprints and manages the Rap Back Service transactions on behalf of the subscriber. The subscriber and the submitter must establish a secure and effective communications infrastructure to manage the Rap Back subscriptions and to coordinate with the CJIS Division. In some instances, both the submitter and the subscriber will be the same government agency.

The Rap Back Guide includes an Appendix II that serves as a participation plan for subscribers, submitters, and the CJIS Division. This document outlines compliance with all requirements for participation in the Noncriminal Justice Rap Back Service. These requirements include training of personnel, auditing, Electronic Biometric Transmission Specification (EBTS)⁶ compliant fingerprint submissions, and ongoing record and subscription validation. Subscribers are responsible for validating their Rap Back subscriptions in a timely manner to ensure they remain in an authorizing relationship with the subscribed individuals. This means certifying that the individual is still licensed,

³ See: 28 CFR 20.3(i) for examples of dispositions within this definition.

⁴ See: <https://www.fbi.gov/file-repository/pia-next-generation-identification-latent-services.pdf/view>

⁵ An SIB is a state governmental agency responsible for criminal fingerprint identification services and submitting fingerprints and Rap Back subscriptions to the NGI System for jurisdictions within the state not served by federal agencies or authorized contractors. <https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/identity-history-summary-checks/state-identification-bureau-listing>.

⁶ EBTS is the required technical specification for submission of biometrics to the NGI System. The most recent document version can be located at <https://fbibiospecs.fbi.gov/ebts-1/approved-ebts>.

employed, volunteering, or is otherwise continuing a relationship with the subscriber that authorizes under law or regulation the subscriber to receive CHRI. For example, if a person has changed occupations or retired, the subscriber must notify the submitter to remove the subscription from the Rap Back Service within five business days of the final determination of the subscriber no longer having the authority to continue monitoring the individual.

When a subscriber uses a contractor to act as the submitter, this separate entity is referred to as a channeler. A channeler may be a government agency, a private business, or a nonprofit organization that is not itself an authorized recipient, and that has entered a contract with the authorized recipient for this purpose. A channeler is approved by the FBI to obtain a direct connection to the NGI System for the purpose of electronic submission of fingerprints and the receipt of CHRI on behalf of an authorized recipient⁷. In addition, a contractor known as a non-channeler is a government agency, a private business, or a nonprofit organization that has entered a contract with the authorized recipient to perform administrative functions for the authorized recipient, such as storing or adjudicating CHRI. A non-channeler is not a submitter and does not have a direct connection to the NGI System. The NGI Noncriminal Justice Rap Back Service Outsourcing Policy and Implementation Guide (Rap Back Outsourcing Guide) provides requirements for channelers and non-channelers that assist a subscriber or submitter with participation in the Rap Back Service.

All subscribers to the Rap Back Service must choose a Privacy Risk Mitigation Strategy (PRMS) listed in the Appendix II to protect individual privacy rights, maintain the integrity of the Rap Back Service, and ensure accuracy of the NGI System. The five PRMSs were approved and are governed by the National Crime Prevention and Privacy Compact Council (Compact Council)⁸. An authorized agency may choose:

- (1) *Pre-Notification*: The subscriber must confirm the authorizing relationship with the fingerprinted individual prior to receiving the CHRI or other triggering event information from the Rap Back Service. If pre-notification is used, the subscriber is not required to validate records, including the ongoing authorizing relationship, before 5 years;
- (2) *Authority for the Duration of License*: The expiration of the Rap Back subscription is set for the time period of the professional license; however, the subscriber still must validate records within five years of the subscription;
- (3) *Statutory or Regulatory Authority for Set Term*: The expiration of the Rap Back subscription is set for the time period permitted by the relevant legal authority; however, the subscriber still must validate records within five years of the subscription;
- (4) *One-Year Validation or Expiration*: For any Rap Back subscription, a one-year validation of records or one-year mandatory expiration date is sufficient; or
- (5) *Subscription Synchronization through Automated or Formalized Procedures*: Subscribing

⁷ See *Compact Council: Security and Management Control Outsourcing Standard for Channeling* which outlines the individual and collective responsibilities of the parties involved in an outsourcing agreement, so that the security and integrity of the NGI System and CHRI are not compromised. <https://www.fbi.gov/file-repository/compact-council-security-and-management-control-outsourcing-standard-for-channelers.pdf/view>.

⁸ The Compact Council was created pursuant to the National Crime Prevention and Privacy Compact Act of 1998, Title 42 U.S.C. Chapter 140, to facilitate the exchange of authorized interstate criminal history records for noncriminal justice purposes. The FBI is a member of the Compact Council.

entities are required to maintain synchronized records with the NGI System, with strict controls, and to conduct formal validation at a minimum of every five years.

Pursuant to the Rap Back Outsourcing Guide, channelers and non-channelers must use pre-notification as the PRMS and perform a mandatory validation of records within one year. Otherwise, subscribers may choose to use different PRMSs for different populations. For example, realtors within a state may be subscribed for the duration of a license, police officers may be subscribed with one-year validation, and nurses may be subscribed with pre-notification. If a subscriber needs to add new populations to the Rap Back Service, it can file an Addendum with the CJIS Division identifying the new population and outlining the legal authority for submission. Regardless of the PRMS chosen, all records must be validated within five years of the Rap Back subscription being set. If the subscriber fails to verify continued authorization, the Rap Back subscription will expire automatically.

Criminal Justice Rap Back

Law enforcement agencies, probation and parole officers, and other criminal justice entities are authorized to use the Criminal Justice Rap Back Service for notification of potential subsequent criminal activity of persons under their supervision or under active criminal investigation. Populations may include probationers, parolees, sex offenders, and those under orders related to immigration enforcement, such as orders of removal or deportation. The NGI Criminal Justice Rap Back Policy and Implementation Guide (Criminal Justice Rap Back Guide) provides the policy, legal, privacy, and security requirements for agencies that participate in the Criminal Justice Rap Back Service. It is important to note that criminal justice agencies have pre-existing access to the NGI System to perform the administration of criminal justice, and the administration of criminal justice includes the collection, storage, and dissemination of CHRI.⁹ Criminal Justice Rap Back subscriptions may only be established by recognized criminal justice agencies with an existing Originating Agency Identifier Number (ORI)¹⁰ assigned by the CJIS Division. A criminal justice agency may not establish a Rap Back subscription unless it is authorized under current FBI 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. In other words, the criminal justice agency must already be authorized to access the individual's CHRI in the NGI System to establish a subscription within the Criminal Justice Rap Back Service.

Investigative subscriptions may only be established for criminal cases that have been assigned an official agency case number by the subscriber and for which the statute of limitations has not expired. All investigatory Criminal Justice Rap Back subscriptions must include the subscriber's case number which is entered in the originating case number (OCA) field within the EBTS transaction; otherwise, the subscription will be rejected. The purpose of the OCA requirement is to assist the CJIS Division with confirmation that the investigative subscription is supported by an official, open law enforcement investigation.¹¹

⁹ See 28 CFR 20.3(b): the administration of criminal justice consists of detection, apprehension, detention, pretrial and post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders, and criminal identification activities.

¹⁰ An ORI is a unique number that is assigned to each agency authorized to access the NGI System and controls the level and type of access.

¹¹ OCAs can be audited by the FBI audit unit or CJIS Systems Officers to ensure proper use of the system, as discussed in sections 6.2 and 8.

To participate in the Criminal Justice Rap Back Service, criminal arrest fingerprints must be submitted for retention or already be retained within the NGI System. A probationer, parolee, or otherwise supervised person should have pre-existing criminal fingerprints in the NGI System. To receive notification of subsequent activity, the authorized agency simply subscribes to the fingerprints currently in the NGI System using the individual's UCN. However, some individuals under criminal investigation may not have fingerprints retained in the NGI System. In that instance, the authorized agency must submit fingerprints prior to, or in conjunction with, a Rap Back subscription enrollment. Criminal Justice Rap Back subscriptions may not be established on civil fingerprints in the NGI System.

Consistent with Noncriminal Justice Rap Back, all established Criminal Justice Rap Back subscriptions will include electronic notification of any subsequent arrest of the individual and any identity maintenance which may occur including identity deletion, restoration, and/or consolidation. In addition to arrest and identity maintenance notifications, the Criminal Justice Rap Back Service provides notice of other "triggering" events chosen by the authorized agency. These triggering events are the same as those described above for the non-criminal justice agencies. By default, all Criminal Justice Rap Back subscriptions have a mandatory expiration date. For supervisory subscriptions, the maximum subscription term is five years. For investigative subscriptions, the maximum subscription term is one year, with the agencies being advised to set the Rap Back subscriptions to the shortest time period necessary for the investigation. Both supervisory and investigative subscriptions may be extended if actively re-validated by the subscriber.

2.2 *Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)*

Authority	Citation/Reference
Statute	8 U.S.C. §1722; 28 U.S.C. §§ 533, 534; 42 U.S.C. § 3771; 44 U.S.C. § 3301
Executive Order	E.O. 8781, 8914, 10450, 13356, 13467
Federal regulation	28 CFR §§ 0.85, 20.31, 20.33, Part 907
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 *Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in*

Department of Justice Privacy Impact Assessment
Federal Bureau of Investigation/NGI Rap Back Services

Page 7

Column (2) and indicate to whom the information relates in Column (3). *Note: This list is provided for convenience; it is not exhaustive. Please add to “other” any other types of information.*

The Noncriminal Justice Rap Back Service requires the same information that is collected with all retained civil fingerprint submissions to the NGI System. In addition to the civil fingerprints, mandatory biographic information includes name, date of birth, place of birth, and sex. A Criminal Justice Rap Back subscription may be set on newly submitted criminal fingerprints or existing criminal fingerprints retained in the NGI System. Additional required information includes the UCN, name, and date of birth.

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

Department of Justice Privacy Impact Assessment
Federal Bureau of Investigation/NGI Rap Back Services

Page 8

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Employment status, history, or similar information	X	A, B, C, D	
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, D	
Juvenile criminal records information	X	A, B, C, D	As permitted by state and federal law
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
<i>Biometric data:</i>			
- Photographs or photographic identifiers	X		May be retained as a supplementary biometric with a criminal identity in the NGI System but not used for Rap Back enrollment, maintenance, or dissemination.
- Video containing biometric data			
- Fingerprints	X	A, B, C, D	

Department of Justice Privacy Impact Assessment
Federal Bureau of Investigation/NGI Rap Back Services

Page 9

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- Palm prints	X		May be retained as a supplementary biometric with a criminal identity in the NGI System but not used for Rap Back enrollment, maintenance, or dissemination.
- Iris image	X		May be retained as a supplementary biometric with a criminal identity in the NGI System but not used for Rap Back enrollment, maintenance, or dissemination.
- Dental profile			
- Voice recording/signatures			
- Scars, marks, tattoos	X		May be retained as a supplementary biometric with a criminal identity in the NGI System but not used for Rap Back enrollment, maintenance, or dissemination.
- Vascular scan, e.g., palm or finger vein biometric data			
- DNA profiles			
- Other (specify)			
<i>System admin/audit data:</i>			
- User ID	X	A	
- User passwords/codes			
- IP address	X	A	
- Date/time of access	X	A	
- Queries run	X	A	
- Contents of files			
Other (please list the type of info and describe as completely as possible):	X	A, B, C, D	Unique identifying numbers such as UCN

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

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

Government sources:			
Within the Component	X	Other DOJ Components	X
		Other federal entities	X

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

Nongovernment sources:				
Members of the public		Public media, Internet		Private sector X
Commercial data brokers				
Other (specify) Private sector refers to the approved contractors (i.e., channelers and nonchannelers) that submit fingerprints to the NGI System and perform other Rap Back Service tasks on behalf of the subscribers.				

Section 4: Information Sharing

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

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct log-in access	Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.
Within the Component			X	
DOJ Components			X	
Federal entities			X	
State, local, tribal gov't entities			X	
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector			X	Approved contractors that submit fingerprints and perform other non-criminal Rap Back Service tasks on behalf of the subscribers.
Foreign governments				

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct log-in access	Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.
Foreign entities				
Other (specify):				

4.2 *If the information will be released to the public for “[Open Data](#)” purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.*

N/A.

Section 5: Notice, Consent, Access, and Amendment

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

For the Noncriminal Justice Rap Back Service, when fingerprints and associated biographic information are collected from an individual to establish a Rap Back subscription, the individual must be provided with an FBI Privacy Act notice which addresses the retention and the continual searching of the fingerprints in the NGI System, including the latent repository. In addition to the Privacy Act notice, individuals must receive a notice that contains the requirements of 28 CFR 50.12, “Exchange of FBI identification records”. This regulation includes requirements to notify individuals of the use of their fingerprints to search the criminal history records of the FBI, and the right of individuals to access and challenge their criminal history records maintained by the FBI.

The Privacy Act and 50.12 notices were approved by the Compact Council and are documented requirements in the Appendix II of the Rap Back Guide. The subscriber must specifically identify in the Appendix II participation plan how the Privacy Act and 50.12 notices will be provided to new applicants as well as legacy populations for whom fingerprints have already been retained within the NGI System. The subscriber’s process for providing the Privacy Act and 50.12 notices must be approved by the FBI Privacy and Civil Liberties Unit and is audited by the CJIS Division.

For the Criminal Justice Rap Back Service, the FBI has exempted itself from the requirement of 552a(e)(3) for the criminal and national security records maintained in the NGI System. However, the NGI System’s SORN provides general notice of the collection and use of criminal fingerprints, and the most current version may be found at 84 Fed. Reg. 54,182 (October 9, 2019). This PIA also provides general notice, as does the previously published PIAs regarding the NGI System, which may be found at <https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments>.

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

Individuals voluntarily provide their fingerprints to authorized agencies for submission and enrollment in the Noncriminal Justice Rap Back Service for noncriminal justice purposes, such as employment, security clearances, or immigration benefits. The individual is informed of the FBI's uses of the information with the specific FBI Privacy Act notice required for Noncriminal Justice Rap Back participation. An individual whose fingerprints were collected in connection with a criminal arrest or investigation has no opportunity to refuse the collection of his or her personal information. Nevertheless, criminal justice uses of the information in the NGI System must comply with the provisions of applicable law, including the Privacy Act.

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

Individuals do not have access to information retained or disseminated by the Rap Back service. If an individual wishes to remove themselves from the recurrent vetting of non-criminal Rap Back Service they must work through the original submitting agency to request removal. Title 28 CFR part 16, subpart A, provides general guidance on access to information in FBI files pursuant to the Freedom of Information Act; and 28 CFR part 16, subpart D, provides general guidance regarding access to, and amendment of, information in FBI files pursuant to the Privacy Act. Title 28 CFR 16.30-16.34 establish specific procedures for an individual to obtain a copy of his or her criminal history record from the NGI System for review and correction. Note: the FBI maintains exemptions from access and amendment provisions of the Privacy Act for certain records maintained in the NGI System.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO): January 9, 2023, to January 8, 2026. If an ATO has not been completed, but is underway, provide status or expected completion date: Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation: No POAMs related to privacy controls.
---	---

	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information, and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan: Confidentiality: high; Integrity: high; Availability: high. The NGI System is high across all categories on two grounds. The first is that law enforcement officer safety requires access to this information in a timely and accurate manner. The second is that public privacy requires confidentially be maintained to those members of the user community with the need to know this information.
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: The NGI System is continually monitored at the host and network layer. FISMA policy compliance testing occurs monthly.
X	Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted: Host operating system logs are consolidated into the CJIS enterprise system audit consolidation and monitored for irregular activities or compliance failures. The NGI System Security Administrator reviews security-related logs on a weekly basis.
X	Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy.
X	Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe: Users receive security/privacy training as an initial requirement of access to the NGI System, and annually thereafter. The participating Rap Back agencies are required to provide continuous training to their employees. The Rap Back team provides overviews, assists with the Appendix II, and coordinates necessary testing prior to participation.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

The primary transmission method of biometric submissions to the NGI System, including fingerprints for the Rap Back Service, is electronically via the CJIS wide area network (WAN). The CJIS WAN is a telecommunications infrastructure that connects authorized agencies to the NGI System and other host computer systems. The CJIS WAN provides a secure transport mechanism that supports the exchange of encrypted CHRI and biometrics. The CJIS WAN is configured by FBI personnel and

secured through firewall mandates. Biometric submissions may also be transmitted to the NGI System via a Virtual Private Network (VPN). When connected to a VPN server, an encrypted tunnel is created for internet traffic. The data transmitted between the submitter's device and the VPN server is scrambled, becoming unreadable to any third parties that might be trying to intercept it, such as hackers, internet service providers, or other entities. This encryption process essentially wraps the data in a protective layer, ensuring that sensitive information and communications remain private and secure as they travel across the internet. This encryption ensures that even if the data is intercepted, it cannot be read by unauthorized parties. At this time, all channelers submitting Rap Back subscriptions use the VPN option; the government agencies generally submit transactions via the CJIS WAN.

Alternatively, the use of the Galton Software Suite (Galton) has been approved for federal agencies, including the FBI's Security Division, that have a direct connection to CJIS. Galton submits EBTS compliant fingerprints using a hypertext transfer protocol secure (HTTPS) connection to access the NGI System. Galton submits the EBTS file via secure Web services, utilizing HTTPS and Transport Layer Security 1.2. Galton also has a unique dashboard that allows authorized agencies to perform maintenance and cancellations for Rap Back subscriptions.

As discussed, fingerprints submitted to establish Rap Back subscriptions must comply with the EBTS. The EBTS ensures compatibility with the NGI System and extends beyond the American National Standards Institute/National Institute of Standards and Technology - Information Technology Laboratory (ANSI/NIST-ITL) standard. ANSI/NIST-ITL is developed and maintained in conjunction with the National Institute of Standards and Technology and the biometric community. While the ANSI/NIST-ITL standard provides guidelines for the exchange of information between various local, state, tribal, federal, and international biometric systems, the EBTS defines requirements to which agencies must adhere when electronically communicating with the NGI System.

The NGI System provides access and authentication to system level information based upon the authorized General User (contributor) and Privileged User (system administrator) access and as defined within the NGI System's User's Guide. Privileged Users are provided with capabilities to view submission data for purposes linked to administration of the NGI System. All General User and Privileged User actions are logged in the system audit logs with full traceability to individual users performing actions. All system audit logs are retained in accordance with FBI retention policies and guidelines. General Users of the NGI System and corresponding capabilities are controlled through agency agreements according to the CJIS Security Policy and vetted by the individual federal and state agency CJIS Systems Officers (CSOs). Rap Back Service users must ensure compliance with the CJIS Security Policy and applicable CJIS User Agreements. Rap Back subscriptions may only be established by a government agency or a nongovernmental entity that has been assigned an ORI by the CJIS Division.

The CJIS Security Policy governs the security information requirements for all CJIS Systems, including the NGI System, and controls include security training, reporting of security incidents, access control, media protection, and physical and personnel security. The CJIS User Agreement specifies the ways in which each agency - CJIS and each user agency - is responsible for appropriate security measures as applicable to physical security of terminals and telecommunications lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security; dissemination and logging; and security of records. With the NGI System security requirements, dissemination of information is linked to the authorized agency that

requested the information. The NGI System stores information regarding dissemination, such as date, time, and requester in audit logs. Risks are also mitigated by training and by periodic audits conducted by the FBI to ensure system searches are relevant and necessary to the person's official duties.

The CJIS Division has an established Audit Unit that regularly reviews implementation of FBI requirements by agencies that are authorized to access the NGI System. The CJIS Division performs triennial audits of all CJIS system agencies (CSA), the agencies that are responsible for federal or state connections to the NGI System and whose CSOs are responsible for implementing compliance. The CJIS Audit Unit reviews Noncriminal Justice Rap Back Service agencies to ensure compliance with the Appendix II of the Rap Back Guide. The CJIS Audit Unit also reviews the Criminal Justice Rap Back Service agencies to ensure proper authorization to enroll individuals and that subscriptions are removed within the required timeframe.

The state or federal CSOs also are required to conduct audits of their agencies on a triennial basis. The state or federal CSO is responsible for implementing and ensuring compliance with the CJIS Security Policy. The CJIS Division provides training assistance and up-to-date materials to each CSO and periodically issues informational letters to notify authorized users of administrative changes affecting the system. CSOs at the federal and state level are responsible for the role-based training, testing, and proficiency affirmation of authorized users within their respective state or federal agencies. All users must be trained within six months of employment and biennially re-tested hereafter. The CJIS Division and CSA audits confirm that only authorized agency personnel are accessing the NGI System for authorized purposes.

The NGI System is not available to users unless there has been an application for, and assignment of an ORI. Each using entity may only access the types of information for the purposes that have been authorized for its ORI. Such access is strictly controlled and audited by the CJIS Division. Federal and state CSOs must apply to the CJIS Division for the assignment of ORIs and CJIS Division staff evaluates these requests to ensure the agency or entity meets the criteria for the specific type of ORI requested. The CJIS Division maintains an index of ORIs and logs each dissemination of identification records to the applicable ORI.

In addition, the NGI System's Information System Security Officer is responsible for ensuring that operational security is maintained on a day-to-day basis. Adherence to roles and rules is tested as part of the security certification and accreditation process. All FBI employee and contractor personnel must complete privacy training and annual information security training. The training addresses the roles and responsibilities of the users of FBI systems and raises awareness of the sensitivity of the information contained therein and how it must be handled to protect privacy and civil liberties.

In accordance with 28 U.S.C. §534, the FBI does not disclose information from the NGI System outside of the authorized receiving agency or related agencies. Although this is a separate statute from the Privacy Act of 1974, it provides specific controls on the dissemination of CHRI, 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 and users of the Rap Back Service must comply with the Rap Back Guide, the Criminal Justice Rap Back Guide, and the Rap Back Outsourcing Guide.

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

The retention of records in the NGI System is subject to the requirements of the Federal Records Act, administered by the National Archives and Records Administration (NARA). NARA has approved the destruction of fingerprint cards and associated information, including other biometrics, when criminal and civil subjects attain 110 years of age. NARA has determined automated FBI criminal history information and NGI System 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.

Section 7: Privacy Act

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

_____ No. X Yes.

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

The Next Generation Identification System, 81 Fed. Reg. 27284 (May 5, 2016), amended by 82 Fed. Reg. 24156 (May 25, 2017) and 84 Fed. Reg. 54182 (October 9, 2019).

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- *Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),*
- *Sources of the information,*
- *Specific uses or sharing,*
- *Privacy notices to individuals, and*
- *Decisions concerning security and privacy administrative, technical, and physical controls over the information.*

As discussed in Section 2, participation in the Rap Back Service for noncriminal 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 against criminal (including latent) and noncriminal justice fingerprints subsequently submitted to the NGI System. There is a risk that civil applicants may be unaware of the enhanced retention and searching of their fingerprints. This risk is mitigated by the required FBI Privacy Act notice on the FD-258 hard-copy fingerprint cards, electronic live scan devices, or via other electronic or paper means. The Privacy Act notice advises applicants of the authorities for the collection and retention of fingerprints, how the fingerprints will be searched in the NGI system, and how their information may be shared. The Rap Back Service creates no new authority for the submission of civil fingerprints. Each potential participating agency must rely on its existing legal authority or obtain legal authority to submit, retain, and search fingerprints in the NGI System. These legal authorities, this PIA, the NGI SORN, and other official FBI public communications provide notice of the Rap Back Service to the civil applicants.

Participation in the Rap Back Service for noncriminal justice purposes also creates risks that triggering event information and/or personally identifiable information will be disseminated to unauthorized recipients or that subscriptions will remain in the NGI System when the agency no longer has the authority to receive information about an individual. For example, if an individual is no longer employed in a relevant position, the subscribing agency may no longer have the authority to receive information regarding the former employee. To mitigate these risks, each Rap Back subscription must incorporate one of the five PRMS described in Section 2 to ensure continued authorization to receive CHRI and related 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 of the subscription to receive the specific triggering event information. Validation and expiration dates ensure the Rap Back subscriptions do not become stale even if those records are never accessed due to triggering events. Should an individual retire or leave employment for any reason, it is incumbent upon the subscriber to notify CJIS of the change in status. The relevant subscription will then be reviewed and removed from the Rap Back Service by CJIS within five business days of the final determination that the subscriber no longer has authority to monitor the individual. Subscribers establish this process in their Appendix II submissions, and compliance is audited by CJIS. The CJIS Division assists agencies with keeping their Rap Back subscriptions up-to-date and accurate by providing monthly reports of the current enrollments in the NGI System for reconciliation and validation against the agency enrollments. These monthly reports are provided via secure electronic communications. The CJIS Division also alerts agencies when Rap Back subscriptions are nearing their expiration dates to provide the agencies with an opportunity to remove or re-enroll the subscriptions. It is important to note that the maximum time a Noncriminal Justice Rap Back subscription can remain in the NGI System without validation by the submitting agency is five years. At that time, the submitting agency must confirm that the subscription should remain established in NGI, or it will be removed automatically.

Participation in the Noncriminal 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 a variety of ways. Before an authorized agency may submit Rap Back subscriptions to the NGI System, the agency must coordinate with the CJIS Division to complete the Appendix II including

policy, security, and privacy requirements for establishing and managing subscriptions. The completion of the Appendix II gives the CJIS Division an opportunity to ensure the participating agency fully understands the Rap Back Service requirements and is following the necessary processes to assist with mitigating risks.

Training and auditing continue to be integral components to protect against improper access to or use of the Rap Back subscription data. As discussed in section 6.2, above, CJIS has an established Audit Unit that regularly visits subscribers, submitters, and other entities authorized to collect and submit fingerprints for retention in the NGI System. Allegations of misuse of the NGI System are generally referred to the appropriate CSO of the jurisdiction where the misuse occurred, and the FBI responds to all such allegations. For those occasions when records maintained in the NGI System are wrongfully accessed or disseminated, both the CJIS Advisory Policy Board and the Compact Council have established Sanction Committees to address the possible misuse. Finally, the NGI System stores 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.

As discussed above in Section 2, both Noncriminal Justice and Criminal Justice Rap Back subscriptions may only be established by agencies or entities that have been assigned an ORI by CJIS. Therefore, Noncriminal Justice Rap Back subscriptions allow only government agencies or nongovernmental entities that have been authorized by federal statute, federal executive order, or state statute to have access to Rap Back information. For Criminal Justice Rap Back subscriptions, only agencies that would be authorized to conduct criminal inquiries 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 the NGI System for civil purposes. At least one fingerprint-based criminal event must exist before a criminal justice subscription may be permitted. Investigative criminal justice subscriptions may only be established on identities associated with an open law enforcement investigation and must provide the specific agency case number. Likewise, as discussed above in Section 2, 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 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.

The retention of additional data supporting NGI's Rap Back Service also presents a correspondingly increased risk that the FBI will be maintaining more information subject to loss or unauthorized use. Notably, the existing NGI System security requirements and user rules regarding access and dissemination of CHRI remain unchanged with the implementation of the Rap Back Service. The risk of loss or unauthorized use is mitigated by the strong system, user, site, and technical security features present in the NGI System. Another privacy risk could be maintenance of erroneous data within the Rap Back Service. The privacy risk of maintaining erroneous data is mitigated 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 it may become aware. Additionally, this risk is mitigated because the maintenance and dissemination of information must comply with the provisions

of any applicable law, regulation, or policy, including the Privacy Act. Among other requirements, the Privacy Act obligates the FBI to make reasonable efforts to ensure the information that it disseminates to non-federal agencies is accurate, complete, timely, and relevant. FBI relies on the overall NGI system architecture to ensure that Rap Back disseminations are accurate. This risk is further mitigated to the extent that an agency that contributes information to NGI has a process in place for access to or correction of its source records.