Federal Bureau of Investigation

Privacy Impact Assessment
for the
Next Generation Identification System
Repository for Individuals of Special Concern 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: November 7, 2024

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 Repository for Individuals of Special Concern (RISC) PIA published in January 2012.[1] This PIA provides updated information regarding the RISC Service managed by the FBI's Criminal Justice Information Services (CJIS) Division.

The RISC Service permits searching of a subset of identity records maintained in the Next Generation Identification (NGI) System[2] for the purpose of identifying persons who may present heightened risk to the safety of the public or law enforcement personnel. These identity records are queried by fingerprints electronically submitted by authorized NGI System users, typically by state, local, or tribal law enforcement officers during their interaction with potential offenders or similar real-time encounters. The RISC Service permits law enforcement personnel in field settings to use a mobile fingerprint-based search capability to assess the identity and/or threat of an encountered individual. This PIA further addresses the expansion of the RISC Service to provide users with the option to search all identities maintained in the NGI System's Criminal Identity Group.[3] This enhancement will provide RISC users with additional information to assist with identification and other investigatory purposes.

Section 2: Purpose and Use of the Information Technology

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

The RISC Service provides state, local, or tribal law enforcement officers with a mobile fingerprint search capability that can be used in time-critical situations involving heightened investigative interest or increased risk to the public and/or to law enforcement personnel. Currently, the RISC Service searches a subset of criminal identity records maintained in the NGI System that includes known or appropriately suspected terrorists; wanted persons, including both felony and misdemeanor warrants; immigration violators; violent persons; and registered sex offenders.

Prior to participating in the RISC Service, a law enforcement agency must enter a CJIS User Agreement with the CJIS Division. This User Agreement provides the foundational requirements for

---

[1] *See* https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments
[2] The NGI System serves as the FBI's national criminal history and biometrics repository and maintains criminal history record information positively associated with criminal tenprint fingerprints.
[3] The Criminal Identity Group within the NGI System maintains the identities of those persons whose fingerprints have been submitted to the NGI System pursuant to arrest, incarceration, or similar criminal justice purposes.

access to all CJIS Systems, including the NGI System. It establishes the policy, technical, and security requirements for access, including compliance with the CJIS Security Policy. The User Agreement must be signed by the CJIS Systems Officer (CSO) or appropriate state official. The User Agreement also incorporates the Policy and Implementation Guides relevant to specific services, such as RISC. As such, it includes the RISC Implementation Guide that provides law enforcement users with the detailed participation guidance for the RISC Service. In addition to technical and security requirements, the RISC Implementation Guide states that state, local, and tribal law enforcement users must ensure that they adhere to the laws of their jurisdictions and protect the Constitutional rights of all those encountered. Importantly, users are also advised that RISC responses cannot serve as the sole basis for law enforcement action; additional identity confirmation/investigatory actions must be taken. User agencies voluntarily participate in the RISC Service and need to procure the necessary software, certified mobile fingerprint capture devices, and infrastructure to provide their law enforcement officers the ability to perform mobile fingerprint collection and transmit these images to the NGI System. Law enforcement agencies are responsible for assigning its own users under its own policies.

A RISC query of the NGI System is conducted solely with 2 to 10 rolled or flat fingerprint images captured by a certified mobile fingerprint device.[4] No other information regarding the individual, such as physical descriptors or event information, is sent to the NGI System. RISC fingerprint submissions must also include the user agency's originating agency identifier (ORI),[5] the type of fingerprint transaction (i.e., mobile criminal inquiry), the date, and the transaction number. Users may choose to program their mobile devices with optional information such as the user's name, badge number, or telephone number; however, this information is not searched or retained in the NGI System.

The fingerprints are transmitted wirelessly to the law enforcement user's State Identification Bureau or CJIS Systems Agency (CSA), the law enforcement agencies that are responsible for their agency's connections to the NGI System and compliance with the CJIS User Agreement. The user's agency electronically submits the fingerprints to the NGI System via the secure CJIS Wide Area Network (WAN) to conduct a search. 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 criminal history record information (CHRI)[5] and biometrics.

The RISC Service performs "lights-out" processing using fewer than ten fingerprints. Lights-out processing refers to the system completing the search and response functionality automatically. The results of RISC searches are generated within seconds of the submission and responses are returned electronically, within seconds, via the WAN to the submitting agency. The submitting agency forwards the response to the user's mobile device through its own communication channels. The search responses from the NGI System are "red," "yellow," "green," or "reject."

A red response is a hit, indicating identification of a highly probable candidate. However, a red

---

[4] Certified mobile fingerprint devices are tested by an independent testing agency and capture and transmit fingerprint images in accordance with the NGI System's image quality specifications. *See* https://www.fbibiospecs.gov.
[5] An ORI is a unique number assigned by the CJIS Division to a law enforcement agency that controls the level and type of access to the NGI System.
[5] *See* 28 CFR 20.3(d): CHRI includes arrests, detentions, formal criminal charges, and dispositions.

response is not considered a positive identification, but rather a candidate score from the RISC search indicates a high likelihood of identification. (The term "positive identification" currently is reserved for the results of a complete tenprint search and/or confirmation of a match by trained fingerprint examiners.) As articulated in the RISC Implementation Guide, it is incumbent on the requestor to supplement the RISC response with other information to confirm whether the candidate returned is indeed the person whose fingerprints were submitted.

When a RISC search results in a potential hit, the NGI System will use the Universal Control Number (UCN)[6] to automatically message the National Crime Information Center (NCIC) for additional information related to the individual. A red response will return the following information to the law enforcement officer: the category of hit (e.g., wanted person, sex offender, violent person), the UCN, name, and place of birth. If available, additional information from NCIC such as caution and warning fields will be provided. If the state has programmed its mobile devices for the return of CHRI (i.e., rap sheet) and photos (i.e., mugshots), that information will be returned on the initial RISC response. If not, the law enforcement officer will need to conduct a secondary inquiry of the NGI System. Additionally, every red response includes the caveat from the RISC Implementation Guide that advises the law enforcement officer that he/she is prohibited from relying solely on the RISC search response as the impetus for any law enforcement action.

A yellow response is returned when the probable candidate is within the narrow threshold below the level of confidence established for a highly probable match (red response) and no match (green response). While the potential for a yellow response exists, such a response rarely occurs rarely (i.e., less than one-half of one percent of RISC responses) due to the current algorithm thresholds in the NGI System. The searching of the NGI System and NCIC is performed in the same manner as a red response, and the yellow response to the law enforcement officer contains the same information and caveats as returned for a red response.

A green response indicates no hit (i.e., the fingerprint search did not locate a viable candidate in the search of the NGI System. RISC searches will return a reject response when the quality of the fingerprint submission is too low to be used for searching.

Red, yellow, and green responses to RISC searches include a caveat that the response is based solely on a search of a subset of identity records within the NGI System, and that a negative response does not preclude the existence of responsive records in other biometric or name-based repositories.

All RISC searches cascade a search of the NGI Unsolved Latent File (ULF)[7] within the NGI System, comprised of unknown persons whose latent fingerprints have been retrieved from locations, property, or persons associated with criminal activity or related to criminal justice or authorized national security investigations. The cascaded search of the ULF may take considerably more time than that needed to return a tenprint criminal identity response. The ULF search results are not returned to the RISC submitting agency. Instead, if a RISC search hits on a record in the ULF, only the ULF record submitter will receive notification of a potential match to its ULF submission. The ULF record

[6] The UCN is a unique number assigned to each biometric identity in the NGI System.
[7] Privacy Impact Assessment for the Next Generation Identification Latent Services (Mar. 10, 2022), available at https://www.fbi.gov/file-repository/pias/pia-next-generation-identification-latent-services.pdf/view.

submitter may then further develop this lead as it deems appropriate, which may include contacting and coordinating with the submitting agency of the RISC search.

As noted above, the CJIS Division intends to expand the RISC Service by providing an option for RISC participants to search all identities maintained in the Criminal Identity Group of the NGI System, rather than the current subset of criminal identities. Law enforcement agencies will decide whether to implement this enhancement or to continue searching the limited identities. RISC searches of the Criminal Identity Group will follow the same electronic process as the current RISC searches and will return red, yellow, green, or reject responses as described above.

RISC fingerprint submissions are not added to or otherwise retained in the NGI System. The fingerprints are submitted as a criminal inquiry type of transaction and automatically removed from the NGI operational environment after the search is conducted. As such, RISC submissions do not update the criminal history record of a highly probable match candidate, nor do they create a new criminal identity in the NGI System. A submission remains in the NGI System only for the time needed to complete the searching of the RISC and the Criminal Identity Group. It will take only seconds to process a RISC search (including any cascaded NCIC search and search of the Criminal Identity Group), plus the additional time required for the search of the ULF.

The NGI System generates and retains chronological transaction audit information for each RISC search and each response. If a RISC search results in a ULF hit, the NGI System generates and retains chronological transaction audit information regarding the ULF hit notice sent to the ULF submitter. If a RISC search results in a hit to an identity in the Criminal Identity Group, the NGI System retains chronological transaction audit information regarding the CHRI sent to the RISC submitting agency. Similarly, if a RISC search cascades to the NCIC, NCIC generates and retains chronological transaction audit information regarding the NCIC submission and response. These transaction history logs do not contain fingerprints, do not link to or update any identity records in the NGI operational environment, and only contain minimal transaction information for internal research purposes.

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	28 U.S.C. §§ 533 and 534; 34 U.S.C.A. § 10211; the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. 107-56; the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) , Pub. L. 108-458; the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L.110-53; the Federal Records Act (FRA), 44 U.S.C. § 3301 et seq.
Executive Order	EO 13311; and EO 13388
Federal regulation	28 C.F.R. §0.85; Part 20; and §50.12

Agreement, memorandum of understanding, or other documented arrangement	CJIS Division User Agreement; CJIS Security Policy
Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

RISC users query the NGI System with fingerprints captured by certified mobile fingerprint devices. Currently, the RISC Service searches a subset of data maintained in the NGI System that contains the fingerprint records of individuals who present special risks to the public or law enforcement personnel or who may be of heightened investigative interest. The RISC Service will be expanded to search all identities maintained in Criminal Identity Group, if chosen by the law enforcement agency. RISC responses may include the UCN, the name, and the place of birth. If requested by the user, a photo and CHRI, containing additional biographic information, may be returned. The chart below includes both the information collected/returned on an initial RISC query and information contained within CHRI.

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

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**
Tax Identification Number (TIN)			
Driver's license			
Alien registration number	X	A, B, C, D	If provided by the arresting agency.
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
Personal e-mail address			
Personal phone number			
Medical records number			
Medical notes or other medical or health information	X	A, B, C, and D	NCIC caution and medical indicators (e.g., suicidal)
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices	X	B, C	NGI/CJIS WAN returns the RISC response to the state, local, or tribal agency, that then forwards to the individual user. The mobile ID device (make, model, and serial number) may be listed in the equipment used field on the RISC submission. This is not a mandatory field but agencies that do not populate the field have provided device lists to the RISC Service.
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, and D	Criminal record information is limited to the information listed in the CHRI in NGI
Juvenile criminal records information	X	A, B, C, and D	As permitted by state and federal law

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**
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, and D	
- **Video containing biometric data**			
- **Fingerprints**	X	A, B, C, and D	
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**	X	A, B, C, and D	
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	
- **User passwords/codes**			
- **IP address**	X	A	
- **Date/time of access**	X	A	
- **Queries run**	X	A	
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	A, B, C, and D	UCNs or other unique identifiers

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		Other DOJ Components		Other federal entities	
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): State and local law enforcement officers collect fingerprints using a certified mobile fingerprint device to query the NGI System.					

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

Section 4: Information Sharing

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

interconnected systems, or electronic bulk transfer.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component				
DOJ Components				
Federal entities				

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.**
State, local, tribal gov't entities	X			RISC submissions and RISC responses are exchanged via the CJIS WAN to and from authorized agencies and the NGI System.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

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

Not applicable.

Section 5: Notice, Consent, Access, and Amendment

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

No Privacy Act (Act) notice is provided to individuals regarding the collection, use, and sharing of their criminal fingerprints and associated biometric and biographic information in the NGI System. The FBI has been exempted from the requirement of 552a(e)(3) for the criminal records maintained in the NGI System pursuant to the provisions of 552a(j) and (k) of the Act.

The NGI System's SORN provides general notice of the collection and use of fingerprints and associated information. The most current version may be found at 84 Fed. Reg. 54,182 (October 9, 2019), https://www.govinfo.gov/content/pkg/FR-2019-10-09/pdf/2019-21585.pdf. This PIA also provides notice regarding the collection, use, and sharing of information pursuant to the RISC Service.

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.

The fingerprints used to initiate a RISC search of the NGI System typically will be newly collected in field encounters by law enforcement officers for the user agency's purpose under the user agency's legal authorities and policy and training requirements. The user agency will have the sole responsibility for determining whether to collect the fingerprints and must ensure any such collections and uses are lawful and permissible with Federal law and the user agency's governing authorities. Similarly, whether the collected fingerprints will be retained by the user agency (or by other instrumentality of the user agency's government jurisdiction), will be solely determined by the user agency pursuant to its laws and policies.

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

Title 28 CFR part 16, subpart A, provides general guidance on access to information in FBI files pursuant to the Freedom of Information Act; and 28 CFR part 16, subpart D, provides general guidance regarding access to, and amendment of, information in FBI files pursuant to the Privacy Act. Title 28 CFR 16.30-16.34 establishes specific procedures for an individual to obtain a copy of his or her criminal history record from the NGI System for review and correction. Note, however, that the FBI maintains exemptions from access and amendment provisions of the Privacy Act for certain records maintained in 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):** Next Generation Identity System. ATO authorized on January 9, 2023, and expires on 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:** For the NGI System, confidentiality, integrity, and availability is high across all categories. Law enforcement agencies require access to this information in a timely and accurate manner and confidentially must be maintained to those members of the user community with a 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. Monitoring, testing, and evaluation for NGI RISC is also consistent with FBI technical and cybersecurity requirements.
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:** Pursuant to the CJIS Security Policy, all NGI users receive security/privacy training as an initial requirement of access to the NGI system, and annually thereafter. The CJIS Division provides CSAs RISC training materials. CSAs and user agencies are to ensure (via agency audits) that users are trained in the appropriate use of RISC.

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?

RISC submissions received by the NGI System are compliant with the Electronic Biometric

Transmission Specification (EBTS).[8] The EBTS provides proper methods for external users to communicate with CJIS systems for the transmission of biographic and biometric information. 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 NIST 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. Law enforcement agencies electing to utilize the RISC Service to access the NGI System perform compliance and compatibility testing within the system's non-operational testing environments to identify and resolve programming limitations prior to implementing full operating capabilities. This non-operational testing allows compliance problems to be identified and resolved by CJIS and its partner agencies with no harm caused to the accuracy or integrity of the operational system.

User agencies must enter into the CJIS User Agreement to become an authorized user of the NGI System. The CJIS User Agreement includes the policy, technical, and security requirements of access to the NGI System, and incorporates the requirements of the CJIS Security Policy and the RISC Implementation Guide. The NGI System is not available to users unless there has been an application for, and assignment of access permission via a specific ORI. Each user agency may only access the types of information for the purposes that have been authorized by the assigned ORI. Such access is strictly controlled and audited by the CSA and the CJIS Division. CJIS Systems Officers (CSOs)[9] determine which users will be authorized to initiate RISC submissions, the circumstances under which RISC submissions are permissible, and permissible uses of RISC responses. RISC responses are linked to the authorized agency that requested the information. The NGI System stores information regarding disseminations such as date, time, and requestor in audit logs. All system audit logs are retained in accordance with FBI retention policies and guidelines. The CJIS Division performs triennial audits of all CSAs. The CSOs, in turn, conduct audits of their agencies on a triennial basis. These audits confirm that only authorized users are accessing the NGI System for authorized purposes. System access may be terminated for improper access, use, or dissemination of system records, as defined in the CJIS User Agreement.

The CSOs are responsible for implementing and ensuring compliance with the CJIS Security Policy. Part of this responsibility is ensuring that the certified mobile fingerprint devices used to conduct RISC searches comply with the CJIS Security Policy, including configuration management, device identification and authentication, implementation of mandatory protective software, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware. These security provisions protect the integrity of RISC fingerprint submissions. Agencies must be assigned an ORI by the CJIS Division that authorizes RISC searches. To obtain such an ORI, agencies must ensure that their certified mobile fingerprint devices comply with the CJIS Security Policy.

---

[8] *See*: https://fbibiospecs.fbi.gov/ebts-1
[9] Each CSA has a CSO. The CSO serves as the CSA's primary point of contact for access to CJIS Division systems.

The CSOs are also responsible for ensuring that users are trained in the appropriate use of RISC. The CJIS Division provides up-to-date materials to each CSO and periodically issues informational letters to notify authorized users of administrative changes affecting the service CSOs are responsible for the role-based training, testing, and proficiency affirmation of authorized users within their respective agencies.

As discussed in this PIA, the CJIS Division establishes the use policy and technical requirements for the RISC Service; however, it is also the responsibility of the law enforcement agencies to develop appropriate use policies in accordance with the applicable laws and policies of their relevant governmental jurisdictions. All appropriate use policies must protect the Constitutional rights of all persons. RISC users are solely responsible for complying with applicable laws concerning the retention of RISC fingerprint images collected using their certified mobile fingerprint devices. Typically, these devices have limited data storage capability but may temporarily retain fingerprints until the next time the device is used, at which time any stored fingerprints are deleted. The user agency ultimately decides what and for how long information is retained on the mobile devices.

In addition, the NGI System's Information Systems 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.

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

The National Archives and Records Administration (NARA) records schedule N1-065-10-016 has approved the destruction of fingerprint cards and associated information, including other biometrics, maintained in the NGI System 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, including fingerprints, 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. As stated above, fingerprints submitted via a RISC transaction are not retained in the NGI System; the fingerprints are maintained only for the length of time required to conduct the search.

Section 7: Privacy Act

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

_____ No. __X___ Yes.

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

The NGI System: 81 Fed. Reg. 27,284 (May 5, 2016); 82 Fed. Reg. 24151, 156 (May 25, 2017); 84 Fed. Reg. 54,182 (Oct. 9, 2019), https://www.govinfo.gov/content/pkg/FR-2019-10-09/pdf/2019-21585.pdf.

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.***

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 NGI System users must comply with applicable security and privacy protocols addressed in the CJIS Security Policy and CJIS User Agreement.

Searches of the NGI System using fingerprints submitted from mobile fingerprint devices present a potential risk of misidentification if the fingerprint submission method and RISC search process was less effective in accurately identifying responsive records. Misidentification could result in a false positive or false negative. A false positive mistakenly declares a highly probable or possible match (red response or yellow response); any such erroneous information could be returned to the RISC user, thereby subjecting the individual to unwarranted investigative scrutiny. A false negative mistakenly declares there is no match; any such erroneous information could be returned to the RISC user, thereby possibly thwarting investigative efforts, and posing a safety hazard to the unwarned requestor and/or to the public. The potential for false positive or false negative misidentifications is mitigated by RISC

processes which have proven effective since RISC's deployment in 2012.

To mitigate the risk of misidentification, agencies conducting a RISC search must use a certified mobile fingerprint device. Use of a certified device ensures that quality fingerprint images are submitted to the NGI System. Once fingerprints are received by the NGI System, the NGI System conducts a lights-out search to determine if there is a potential candidate. The NGI System's fingerprint comparison algorithm is highly accurate with an accuracy of greater than 99 percent. Accordingly, the NGI System's fingerprint comparison functionality provides a highly reliable biometric search of the NGI System which reduces the risk of misidentification.

As noted above, RISC responses may include NCIC information. RISC cascade searches of NCIC are accomplished using the UCN from a matched fingerprint record in the NGI System. A cascade search of NCIC via RISC will only return NCIC information when there is link between the UCN in the fingerprint record and the UCN in an NCIC record. Although there remains a conceivable risk of erroneous UCN linkage resulting from human error, system failure, or data corruptions, this risk is considered extremely small because of the CJIS system maintenance standards and audits conducted by user agencies and the CJIS Division. Misidentification risks are also further mitigated by the caveats that are included with all RISC responses. RISC users receive notification that a response is not considered positive identification, is to be considered an investigative lead, and is not to be the impetus for any law enforcement action. Further, RISC users are advised that a RISC search does not preclude a record from existing in other biometric, or name-based repositories.

RISC searches are conducted using only fingerprints that are collected directly from the individual; therefore, he/she has knowledge of the collection. RISC submissions do not include any other biometric or biographic information of the subject. Privacy risks are further mitigated because RISC submissions are not added to or otherwise retained in the NGI System identity records. As such, RISC submissions do not create a cycle on the record of a highly probable match candidate, nor do they create a new identity in the NGI System. A submission's active presence in the NGI System is transitory, lasting only for the time needed to complete the automated searching of the special risk records within the system or the entire Criminal Identity Group. It takes only seconds to process a RISC search (including any cascaded NCIC search and search of the Criminal Identity Group), plus the additional time required for the search of the ULF.

The collection and searching of biometric information present privacy risks that the information will be used for improper purposes, or that there will be improper access to or misuse of the information. This risk is significantly mitigated because RISC users must comply with FBI policies, the CJIS User Agreement, and all relevant laws and policies. In addition, RISC users who are collecting fingerprints have received significant legal training as law enforcement officers and are subject to oversight. Additionally, submitting agencies and RISC users must follow guidance issued by the RISC program.

Finally, the privacy implications of RISC searching the entire Criminal Identity Group are mitigated by FBI policies and NGI System operating requirements which have been implemented to safeguard the security and privacy of personal information, biometrics, and associated responses. As discussed above, the expansion of the RISC Service provides authorized users with a mobile biometric capability to access information that they already have authority to receive.