FBI Records: Freedom of Information/Privacy Act

Privacy Impact Assessment
Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Repository for Individuals of Special Concern (RISC)

I. Introduction

This Privacy Impact Assessment (PIA) addresses the Repository for Individuals of Special Concern (RISC), an extract of data in the Next Generation Identification (NGI)[1] that is collated for the purposes of providing an enhanced capability to identify persons who present special risks to the public or law enforcement personnel or heightened investigative interest. RISC will facilitate faster and easier searches of NGI by authorized users in field settings.

I.1. Background

In developing the NGI, the FBI sought to identify necessary improvements in its biometric collections. As part of this process, the FBI canvassed the user and law enforcement communities for their input on desired changes, enhancements, and new initiatives for the system. From September 2005 through March 2006, over 180 groups representing 1,000 user agencies were asked for suggestions on upgrades. Multiple users recommended the expansion of existing capabilities or the development of new functionality to support rapid biometric searches with fewer than ten fingerprint images in time-

FOIA Index

FOIA Home

Contact Us

Records Available Now
- Hot Topics
- The Vault | Alphabetical List
- Check Status of Your FOIPA Request
- FBI Headquarters Reading Room

Records Available by Request
- Overview
- Sample FOIA Request Letter
- U.S. Department of Justice Form 361, Certification of Identity (pdf)

What Happens After Making a Request
- How Long it Takes to Receive Information
- What You Will Receive
- Appeals

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. Currently NGI ULF searches require separate biometric queries. The cascaded search of the ULF may take considerably more time than the RISC search,[4] and the results will not be returned to the RISC submitting agency. Instead, if a RISC submission 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 submitter may then further develop this lead as it deems appropriate, which may well include contacting and coordinating with the RISC submitting agency.

User agencies will participate in the RISC on a purely voluntary basis. If a user agency opts to submit fingerprints for RISC checks, the agency will need to procure the necessary software, mobile fingerprint capture devices, and infrastructure to provide its law enforcement officers the ability to scan fingerprint images in field settings and transmit these images to the FBI for comparison against the RISC. The information transmitted will be anywhere from two to ten rolled or flat fingerprint images obtained via the mobile fingerprint capture device. The RISC submission will include header information identifying the submitting agency and a unique submission number, but will not include the subject's name or other biographic or event information.

RISC submissions will not be added to or otherwise retained in the NGI identity records. An incoming RISC submission's active presence in the NGI system will be transitory, lasting only for the time needed to complete the automated searching. This will take only seconds for the RISC search itself (including any cascaded NCIC search), plus the additional time required for the slower cascaded search of the ULF.

If a RISC submission results in a ULF hit, NGI will generate a notification to the ULF record submitter advising that a potential match has occurred on their ULF submission and providing the agency identifier and submission number for the RISC submission. NGI will generate and retain chronological transaction audit information for each RISC submission and response. If a RISC submission results in a ULF hit, NGI will generate and retain chronological transaction audit information regarding the ULF hit notice sent to the ULF submitter. Similarly, if the RISC cascades a search to the NCIC, the NCIC will generate and retain chronological transaction audit information regarding the NCIC submission and response.

Section 1.0 – The System and the Information Collected and Stored within the System

1.1 What information is to be collected?

As described above, this initiative does not involve a new collection of information from the persons whose records will be placed in the RISC. The RISC entails a specially collated subset of existing records to permit employment of specialized search techniques, much faster searches of the collated information, and much faster responses to authorized users. The RISC subset will consist of NGI records of known or appropriately suspected terrorists, wanted persons, registered sexual offenders, and other special interest categories warranting more rapid biometric-based responses to inquiring users in time-critical situations involving heightened investigative interest or increased risk to the public and/or to law enforcement personnel.

The fingerprint images used to initiate a RISC check typically will be newly collected in field encounters by law enforcement officers for the user agency's own purposes under the user agency's own mission authorities. As with all biometric submissions to CJIS, the user agency will have the sole responsibility for determining whether to collect these fingerprints and must ensure any such collections and uses are lawful and permissible. Similarly, whether or not the collected fingerprints will be retained by the user agency (or by other instrumentality of the user agency's governmental jurisdiction), will be solely determined by the user agency pursuant to its laws and policies.

CJIS is maintaining fingerprint images submitted during the prototype and rollout phase of RISC. Per the MOUs, at the conclusion of the prototyping phase, CJIS will delete or destroy all fingerprint images received from state identification bureaus. Once fully operational, RISC fingerprint submissions will not be added to or otherwise retained in the NGI records.

Transaction logs are created for all incoming and outgoing RISC transactions. The incoming submission logs contain the transaction data, the name of the officer capturing the fingerprints, the make, model and serial number of the image capture equipment, the request for the rap sheet or photograph when indicated, and the name of the repository to be searched. The outgoing transactions return the aforementioned incoming transaction data to the requester, as well as the FBI number, name, and place of birth when candidates result from the search.

1.2. From whom is the information collected?

Information used to populate the RISC, or that will be accessed via the RISC functionalities, will be obtained from existing NGI and NCIC records relating to those categories of persons identified in subsection 1.1 above. This information will have been collected and submitted to the FBI by federal, state, local, tribal, and some foreign agencies and instrumentalities incident to their lawful mission. Most of the biometric information will have been obtained directly from the subject by the submitting agencies, but some may have been obtained indirectly (such as latent fingerprints obtained from crime scenes). Related biographic and event information may either have been obtained directly from the subject by the submitting agencies, or obtained by the submitting agencies from other sources in the course of investigations or other authorized activities.

The biometric images used to initiate a RISC check typically will be newly collected from persons who are the subjects of field encounters by officers and employees of user agencies incident to authorized activities of these agencies. The user agencies may then opt to forward these biometrics to the NGI for RISC checks. In almost all such cases the biometrics will be obtained directly from and with the knowledge of the subject. The collections will be lawful and permissible under applicable laws and policies of the governmental jurisdiction to which the user agency is subject.

Section 2.0 – The Purpose of the System and the Information Collected and Stored within the System

2.1. Why is the information being collected?

The RISC will collate a subset of existing NGI identity records to permit employment of specialized biometric-based search techniques, much faster searches of the collated information, and much faster responses to authorized users in time-critical situations. The RISC will permit rapid, practicable, biometric-based searches in field settings. The resulting benefits will include greater protection for the public and law enforcement personnel, enhanced investigative support, and reduced impact of law enforcement activities on innocent persons with biographic similarities to persons of investigative interest. Before the RISC, biometric-based searches of NGI required the submission of a full set of ten prints, which as a practical matter could only be captured at the user agency's office, to which the subject would have to be transported following arrest or detention. Identity checks in field settings were thus limited to biographic-based checks (such as name and date of birth) which do not uniquely identify a person and could be unreliable due to misinformation provided by the subject and/or misassociation with persons with biographic similarities.

Transaction logs are kept for auditing and tracking purposes and to meet recordkeeping and disclosure accounting requirements under the Federal Records Act and the Privacy Act. There will be no new use of audit log information pursuant to the RISC initiative.

Fingerprint images are being collected during the prototype phase to allow FBI to conduct reviews of all transactions by human fingerprint specialists to assess the accuracy of responses (see Section 2.3).

2.2. What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

The statutory authority for this initiative is 28 U.S.C. §§ 533 and 534. Supplemental regulatory authorities include 28 C.F.R. § 0.85, part 20, and 50.12. The Attorney General has delegated the

delegated them to the FBI CJIS Division. Additional authorities include 42 U.S.C. § 3771, 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; EO 13311 (amended by EO 13388); EO 13388.

The Federal Records Act (FRA), codified at 44 U.S.C. § 3301 et seq., provides another general statutory basis for the FBI to retain and preserve materials submitted for FBI checks and/or obtained by the FBI in the course of authorized investigative activities, in order to ensure adequate and proper documentation of FBI activities.

Currently, an MOU is executed between the FBI/CJIS and each user agency during the RISC development, testing, and roll-out. The MOU details the processes, conditions, and limitations regarding the transmittal, receipt, storage, use, and dissemination of information relating to this initiative. Eventually, RISC coverage will be incorporated into standing CJIS security standards and operating policies applicable to all CJIS users.

2.3. Privacy Impact Analysis: Given the amount and type of data collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

Privacy risks for the RISC arise from any potential vulnerabilities presented by the new RISC processes. Several such risks have been identified and are addressed below.

There would be a new risk if the RISC method(s) for submitting fingerprints were less effective in accurately identifying responsive records, resulting in an unacceptable percentage of misidentifications. A misidentification could result in a false positive or false negative. A false positive mistakenly declares a probable or possible match; any such erroneous information could be returned to the requestor, thereby possibly 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 requestor, thereby possibly thwarting investigative efforts and posing a safety hazard to the unwarned requestor and/or to the public. Recognizing this risk, the FBI is taking great care in calibrating and adjusting the red-yellow-green thresholds to ensure accuracy while providing enough actionable decisions (red or green) to be beneficial to the officer in the field.[5] For the final NGI RISC solution, the NGI System Requirements Document establishes the following criterion: "NGI shall return the correct candidate a minimum of 98% of the time, when it exists in the RISC repository, as a result of a fingerprint feature search in support of RISC rapid searches." CJIS will continue to monitor the accuracy of RISC searches via periodic sampling and audits throughout the system life cycle.

Furthermore, a RISC search submitted from a mobile device is not designed or expected to take the place of customary booking procedures that utilize tenprint submissions. The FBI will emphasize via piloting MOUs and revisions to security standards and operating policies applicable to all system users that RISC responses are not to be considered "positive" identifications and must be used only as investigative aids together with other investigative processes and information. Moreover, as a counterbalancing benefit, a RISC search will make available biometric-based searches in time-sensitive situations where previously only name-based searches were viable. These biometric-based checks can provide more accuracy than name-based checks alone, reducing the number of erroneous identifications in these situations.

Fingerprint submissions to the RISC may involve fewer than ten fingerprints, and may include "flat" prints rather than "rolled" prints. Regarding identification based on a lesser number of fingerprints, the FBI considers that the system's fingerprint technology and technical capacity has sufficiently progressed to permit extremely accurate association with an existing record based on comparison with an existing ten-print set associated with the record. Similarly, based on recent post-processing analysis of over 500,000 submissions, the FBI has determined flat prints provide sufficient biometric features to permit the identification of a highly probable candidate in the RISC. Moreover, live scanning and scanning fewer than ten fingers contributes to the portability of the capture devices. This facilitates the use of the devices in field settings to obtain the accuracy advantages of biometric-based searches in these settings.

There is a risk that fully automated lights-out responses to RISC submissions will not be as accurate as responses that have been confirmed by fingerprint comparisons conducted by humans, thus resulting in an unacceptable percentage of misidentifications. In an attempt to mitigate this risk, during the RISC rollout, CJIS is conducting follow up review of all transactions by qualified fingerprint staff. These reviews are being documented, and any issues are recorded and reported to ensure accuracy of the fingerprint comparisons. The results of these reviews are being studied, and current post-processing analysis has not identified any "false positive" errors in automated RISC responses to submissions from portable capture devices.

There could be a risk that the process for automatically using an incoming RISC biometric query as the basis to generate a text-based query of NCIC might not be sufficiently reliable to produce an appropriate NCIC query, thereby either missing related records in NCIC that should have been returned or returning another subject's NCIC records. To mitigate this risk, all cascaded NCIC searches are accomplished by using the FNU from the biometric record, so that any NCIC responses will be linked by a unique identifier established from positive biometric identification. Although there remains the conceivable risk of erroneous FNU linkage resulting from human error, system failure, or data corruption, this risk is considered extremely small because of CJIS system maintenance standards and audits conducted by State agencies and the CJIS Division. This risk is mitigated by the caveat provided with all RISC responses notifying the user that the RISC search is only a search of the RISC repository and does not preclude a record from existing in other biometric or name based repositories. Additionally, this risk is further mitigated by guidance currently in MOUs and to be incorporated into standing CJIS security standards and operating policies emphasizing that RISC users should not rely on RISC results alone prior to taking any adverse action against a person.

Similarly, there could be a risk that the process for automatically using an incoming RISC biometric query as the basis to generate a biometric-based search of the ULF might not be sufficiently reliable to produce an accurate result, thereby either missing a related ULF record (false negative) or erroneously returning an unrelated ULF record (false positive). The risk of false negatives is not significant because RISC-based ULF searches provide a new capability but do not supplant any existing capability. If a RISC search returns a false negative, the impact (failure to make the ULF connection based on a field check) will be no different from the current situation (inability to make a ULF field check), and the ULF connection can be made later via any separate opportunities for direct searches of the ULF that might occur. The risk of false positives is mitigated because the ULF results are not returned to the RISC submitter in the field (where erroneous "hits" might subject the affected individuals to unwarranted law enforcement responses during the real-time field encounters). Instead, the ULF results are returned to the ULF submitter as potential matches, to be used in the fullness of time as possible leads for further investigative activity (to include subsequent expert examination to positively confirm or rule out any matches).

An additional privacy vulnerability is present to the extent that the RISC enhanced search and response capabilities provide an increased ability to locate information about a specific person that might not otherwise be discovered as quickly or as efficiently, or might never be discovered at all. Although information in NGI and NCIC will have been lawfully acquired and accessible to authorized NGI and NCIC users, currently that information may be more functionally obscure as a result of users having to separately check multiple systems or encountering longer response times. However, this risk is mitigated by the advantages of being able to move quickly and accurately to locate responsive information about a specific person. This capability permits more complete and timely investigative analysis, including more effective and efficient identification of perpetrators and persons who may present increased threats to the safety of the public and law enforcement personnel. The privacy risk is also mitigated by facilitating a more rapid means to eliminate misidentifications and/or rule out concerns that could adversely impact innocent persons.

Another privacy risk could be the ingestion of records that do not belong in the RISC repository. The possibility of the occurrence of this risk is mitigated by CJIS procedures that ensure that fingerprints of

extracts records based on those flags.

Furthermore, the FBI is developing and implementing the new RISC capabilities only after critical performance parameters have been carefully specified, assessed and confirmed through functional and system requirements analysis and piloting. Effectiveness factors will be developed, monitored, and measured throughout the system life cycle.

Section 3.0 – Uses of the System and the Information

3.1. Describe all uses of the information.

RISC searches will be available only to users authorized to initiate searches of NGI and NCIC for authorized law enforcement or national security purposes. Routine uses for information in NGI are currently promulgated in the System of Records Notice (SORN) for the FBI Fingerprint Identification Records System (FIRS), and routine uses for information in the NCIC are promulgated in the NCIC's SORN.[6] In addition to routine use disclosures, this information may be disclosed under other circumstances authorized by the Privacy Act, including disclosures to those Department of Justice (DOJ) personnel who need the information in the performance of their duties.

The results of RISC searches will be used by law enforcement officers as leads to determine the identity and relevant history of the subject and take appropriate investigatory action, and, if necessary, precautions for his or her own safety.

As discussed in section I above, RISC submissions will cascade searches against the latent fingerprints present in the NGI ULF. If a RISC submission results in a ULF hit, NGI will generate a notification to the ULF record submitter advising that a potential match has occurred on their ULF submission and providing the agency identifier and submission number for the RISC submission. The ULF record submitter may then further develop this lead as it deems appropriate to resolve the pending investigation relating to the latent fingerprint.

The transaction logs are used by the CJIS Audit Unit to conduct recurrent audits to ensure the proper access, use, and dissemination of IAFIS/NGI records.

3.2. Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

No. The RISC process (and any cascaded searching of the ULF and NCIC) only involve biometric-based searches to identify pertinent information that may relate to the specific subjects of the RISC checks.

3.3. How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

The NGI and NCIC encompass substantial processes to ensure accuracy of information. The RISC will comprise a subset of information existing in the parent NGI system and thereby subject to the system's existing data quality standards and operating policies. Under these existing requirements, NGI and NCIC users are responsible for ensuring that accurate and complete biographical information is included in NGI and NCIC submissions and that any associated biometrics meet CJIS quality standards. The CJIS Audit Unit regularly checks representative samples of NGI and NCIC submissions for compliance. In addition, the mobile devices used for RISC submissions must be approved by the FBI and comply with the FBI Electronic Biometric Transmission Specification (EBTS), which defines requirements to which agencies must adhere when electronically communicating with CJIS, helping to ensure the accuracy, image quality, and interoperability of RISC submissions. (See subsection 9.1 below.)

3.4. What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

The National Archives and Records Administration (NARA) has approved the destruction of fingerprint cards and corresponding indices when criminal subjects attain 99 years of age,[7] or seven years after notification of death. NARA has determined automated FBI criminal identification records (rap sheets) and NGI and NCIC transaction logs are to be permanently retained. Biometrics and associated biographic information may be removed from the NGI earlier than the standard NARA retention period pursuant to a request by the submitting agency or the order of a court of competent jurisdiction.

RISC submissions will not be added to or otherwise retained in NGI identity records. An incoming RISC submission's active presence in the NGI system will be transitory, lasting only for the seconds needed for the RISC search itself (including any cascaded NCIC search), plus the additional time required for the slower cascaded search of the ULF. Chronological records of RISC and NCIC submissions and responses (including any ULF hit notices) will be permanently retained in the respective NGI and NCIC transaction logs. (See subsections 1.2 and 1.1 above.)

3.5. Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Please see the discussion in subsection 2.3 above and section 8 below.

Section 4.0 – Internal Sharing and Disclosure of Information within the System

4.1. With which internal components of DOJ is the information shared?

Components of DOJ may make RISC submissions and receive candidate information in the same manner as other state, local, and federal law enforcement partners. This will primarily encompass the following DOJ components whose missions typically involve interactions in field settings with persons associated with criminal activity or otherwise having a lawful investigative or national security interest: the FBI, the Drug Enforcement Administration (DEA), the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the Federal Bureau of Prisons (BOP), the United States National Central Bureau INTERPOL, and the United States Marshals Service (USMS). In addition, any DOJ component that has previously submitted a latent fingerprint to the NGI ULF file will be notified if a RISC submission hits on that latent fingerprint.

4.2. For each recipient component or office, what information is shared and for what purpose?

The results of RISC searches will primarily be given to a submitting component's on-scene employees in real time whenever the subject of the RISC submission may be a wanted person, registered sexual offender, known or appropriately suspected terrorist, or other person of heightened investigative interest or who may present increased risk to the public and/or to law enforcement personnel. In addition, if a RISC submission results in a ULF hit on a latent fingerprint previously submitted by a DOJ component, the submitting component will be notified of the potential match for use as a lead in furthering the investigation involving the latent fingerprint. Authorities for these disclosures include those cited in subsection 2.2 above.

For additional discussion of the contents of RISC responses and the purposes underlying the RISC, please refer to section I, section 2, and subsection 3.1, above.

4.3. How is the information transmitted or disclosed?

The RISC will typically be queried on a case-by-case basis by authorized NGI users incident to real-time encounters in field settings, when two to ten fingerprints may be captured by an FBI-approved mobile fingerprint device and transmitted wirelessly to the user's headquarters and then on to the RISC using existing NGI communications infrastructure.[8] The results of a RISC search will be returned to the submitting headquarters via existing NGI communications infrastructure and may then be wirelessly transmitted back to the field user. If a RISC submission results in a ULF hit on a previously submitted latent fingerprint, the latent-submitting component will be notified of the potential match via existing NGI communications infrastructure.

what privacy risks were identified and how they were mitigated.

Information is disclosed only to DOJ users who have been given authorized access to the information in NGI and the NCIC in accordance with all applicable laws, regulations, SORNs, and long-standing CJIS security standards and operating policies applicable to all system users.

There could be a risk if the technology used for RISC submissions were unreliable, insecure, or incompatible with the RISC processes. To mitigate this risk, mobile devices used for RISC submissions must be approved by the FBI. Additionally, all mobile devices must meet the current CJIS Security Policy requirements including data encryption and advanced authentication. The CJIS Security Policy also contains standards for wireless transmissions that require establishment of usage restrictions and implementation guidance for wireless technologies and authorization, monitoring, and controlling of wireless access to information systems. Once the RISC wireless transmissions reach the submitting agency's headquarters, onward routing of the submission to the RISC will be via existing NGI communications infrastructure incorporating extensive security safeguards.

Please see subsections 2.3 above and 5.4, 5.5, and 5.6 below.

Section 5.0 – External Sharing and Disclosure

5.1. With which external (non-DOJ) recipient(s) is the information shared?

Federal, state, local, tribal, foreign, or international governmental agencies which are authorized access to the underlying information in the NGI and the NCIC and which requires the information in the furtherance of its lawful mission may make RISC submissions and receive candidate information. This will primarily encompass those agencies whose missions involve interactions in field settings with persons associated with criminal activity or related to criminal justice or authorized national security investigations. In addition, any NGI user that has previously submitted a latent fingerprint to the NGI ULF file will be notified if a RISC submission hits on that latent fingerprint.

5.2. What information is shared and for what purpose?

The results of RISC searches will primarily be given to authorized NGI and NCIC users in order to alert a submitting agency's on-scene employees in real time whenever the subject of the RISC submission may be a wanted person, registered sexual offender, known or appropriately suspected terrorist, or other person of heightened investigative interest or who may present increased risk to the public and/or to law enforcement personnel. In addition, if a RISC submission results in a ULF hit on a latent fingerprint previously submitted by a law enforcement agency, the submitting agency will be notified of the potential match for use as a lead in furthering the investigation involving the latent fingerprint Authorities for these disclosures include those cited in subsection 2.2 above.

5.3. How is the information transmitted or disclosed?

The transmission of information is the same as for internal sharing, described in 4.3.

5.4. Are there any agreements concerning the security and privacy of the data once it is shared?

Title 28 U.S.C. § 534 provides that the dissemination of information under its authority is subject to cancellation if shared information is disclosed outside the receiving agency or related agencies. Title 28 C.F.R. § 20.33 provides supplemental guidance regarding the dissemination of criminal history record information, including identification of authorized recipients and possible sanctions for unauthorized disclosures. These restrictions are in turn reflected in longstanding and extensive NGI and NCIC security standards and operating policies applicable to all system users.

In addition, the FBI has entered into RISC-specific MOUs with all participating agencies and similar provisions will eventually be added to CJIS operating policies. These MOUs generally include provisions emphasizing that the RISC searches will be limited to authorized agencies for authorized purposes and that all CJIS rules regarding access to and use of CJIS information apply. Eventually, these provisions will be incorporated into standing CJIS security standards and operating policies applicable to all CJIS users. All authorized NGI users interfacing with RISC will be required to adhere to these same CJIS rules.

Pursuant to the RISC MOUs and/or upcoming CJIS operating polices, the individual federal and state authorities will establish how RISC responses will be disseminated and maintained. For instance, a state may determine that only red and green responses will be forwarded to on-scene users, or before forwarding RISC responses to on-scene users a State may replace the RISC's red-yellow-green terminology with some alternative terminology preferred by the State (such as probable hit-possible hit-no hit). As another example, one state may decide that RISC responses will not be retained in the State records about the subject, whereas another state may decide that RISC responses will be retained in the state records about the subject

5.5. What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

Pursuant to longstanding NGI and NCIC security standards and operating policies applicable to all system users, CJIS Systems Officers at the all government levels are responsible for the role-based training, testing, and proficiency affirmation of authorized NGI and NCIC users within their respective organization. All users must be trained within six months of employment and biennially retested thereafter. When implemented, RISC processes will be incorporated as part of this training. The RISC Program Office provides training to all participating agencies regarding RISC capabilities. The participating agencies are responsible for ensuring training on the use of their wireless devices and the appropriate use of RISC, including the fact that RISC responses do not provide the sole justification for law enforcement action.

5.6. Are there any provisions in place for auditing the recipients' use of the information?

Yes. Please see subsections 8.5 and 8.6 below

5.7. Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and how were they mitigated?

Information is disclosed only to agency users who have been authorized access to the information in NGI and the NCIC in accordance with all applicable laws, regulations, SORNs, and long-standing CJIS security standards and operating policies applicable to all system users.

There would be a risk if the technology used for RISC submissions were unreliable, insecure, or incompatible with the RISC processes. Mitigation of this risk is discussed in subsection 4.4 above

Please see subsections 2.3, 5.4, 5.5, and 5.6 above.

Section 6.0 – Notice

6.1. Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

The user agencies that contribute the underlying information to the NGI and NCIC likely do not provide any sort of Privacy Act Statements or similar actual notice to the individuals from whom or about whom the information pertains. This is because non-federal contributors are not subject to the Privacy Act, federal contributors are usually exempted from the Privacy Act's individual collection notice provisions in connection with criminal law enforcement activites, and/or provision of individual notice incident to criminal law enforcement activities is typically impracticable

General notice regarding the collection of information in the NGI and NCIC has been provided to the public at large via the FIRS and NCIC SORNs. RISC is a subset of NGI, and FBI has provided notice

(JUSTICE/FBI-009) (64 FR 52343, 52347; 66 FR 33558; 70 FR 7513, 7517; 72 FR 3410).

The publication of this PIA will provide general advance notice to the public for all RISC-related collections that will occur subsequent to the publication.

Additional notice might be provided by the federal, state, local, or tribal agency which contributes the underlying NGI and NCIC information and/or which conducts the RISC check.

Even absent any formal notice, for the most part the information in the RISC subset will be based on one or more instances of direct criminal justice processing of the individual (such as "booking") of which the individual will be specifically aware. Similarly, the fingerprints in a RISC submission will have been taken incident to direct involvement with law enforcement in a field encounter of which the individual will be specifically aware their fingerprints are being taken. It is the responsibility of the submitting agency to inform the subject, based on standard operating procedures and appropriate use guidance, of the reason for fingerprint collection. In some situations, such as the conduct of criminal investigations or issuance of arrest warrants, the affected individuals may not always be specifically aware that personal information is being collected and disseminated. However, individuals planning or engaging in criminal activities may reasonably be charged with constructive knowledge that law enforcement will zealously seek to collect and lawfully disseminate all relevant information to identify them and to deter or prevent them from committing crimes.

6.2. Do individuals have an opportunity and/or right to decline to provide information?

Because the information in the RISC subset is collected in connection with law enforcement investigations and/or processing, individuals generally do not have the right or opportunity to object to the collection of this information by the source agencies, nor to the forwarding of the collected information for retention in the NGI and/or the NCIC, nor to the collation of the RISC subset from information in the NGI.

Whether or not individuals will have the right or opportunity to object to the collection of the fingerprints used to initiate a RISC check, and the consequences for objecting, will depend on the location and circumstances of the particular field encounter from which the fingerprints were obtained. All collections must be lawfully obtained under the laws, regulations, and policies to which the agency that obtained the fingerprints may be subject. In many instances the fingerprints for RISC checks may be collected in connection with law enforcement investigations and/or processing in which the individuals generally may not be accorded the right or opportunity to object to the collection. However, in other instances a submitting agency may be obligated under its governing laws, regulations, and/or policies to accord an individual the right or opportunity to object to the collection; personnel of an encountering agency may, in their discretion, voluntarily elect to ask an individual to consent to the collection. In some situations where an individual declines to consent to collection, the encountering agency may nonetheless be entitled to proceed with nonconsensual collection based on alternative authority. In other situations, however, an individual's failure to consent may be controlling, and the encountering agency will have to forego the collection and resolve the encounter without the benefit of a RISC check. Even where an individual is able to successfully decline to be subject to a RISC check, the consequences will vary. In some circumstances a RISC check would not have affected the eventual outcome of an encounter, so the declination will have no consequences to the individual. In other circumstances the results of the RISC check could have altered the outcome of an encounter. This might result in an individual's avoiding further law enforcement interest if the encountering agency were aware of derogatory RISC information (e.g., a "red" or "hit" response), but it could result in an individual's being subjected to prolonged law enforcement interest that might have been avoided if the encountering agency were aware of a non-derogatory RISC response (e.g., a "green" or "no-hit" response).

6.3. Do individuals have an opportunity to consent to particular uses of the information? If such an opportunity exists, what is the procedure by which an individual would provide such consent?

For the same reasons discussed in subsections 6.1 and 6.2 above, individuals generally do not have the opportunity and/or right to consent to particular uses of the information in the RISC subset, since it is obtained from criminal justice subjects incident to criminal justice processes.

To the extent that an individual may have the option to successfully decline to submit to a RISC check as discussed in subsection 6.2 above, the individual would thereby have the opportunity to decline consent and thereby preclude such a use of his/her fingerprints.

6.4. Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The privacy issue present here would be adequacy of notice to affected individuals about how information about them is being collected, maintained, and used, and adequacy of opportunity for the individuals to effectively object to such collection, maintenance, and/or uses. These risks are mitigated by the general notice to the public at large via the FIRS and NCIC SORNs and by the publication of this PIA. Any such collection, maintenance, and/or uses must comply with the provisions of any applicable law, regulation, or policy, including the Privacy Act. Privacy risks are further mitigated to the extent that collecting agencies in some jurisdictions may in certain instances provide actual notice and/or the opportunity to decline to submit to RISC checks. Although availability of such further mitigation will vary depending on the jurisdiction involved, the differences represent an appropriate deference to the principles of federalism.

Section 7.0 – Individual Access and Redress

7.1. What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Pursuant to subsection (j)(2) of the Privacy Act, RISC-related information is exempt from the individual access, accounting and amendment provisions of the Act due to the law enforcement nature of the information. As such, 28 C.F.R. § 16.30-16.34 and 20.34 provide the only means for access and amendment of criminal history records. Under these regulations, a subject of an FBI identification record may obtain a copy of his or her own record for review and correction. If after reviewing his identification record the subject thereof believes that it is incorrect or incomplete in any respect and wishes changes, corrections, or updating, he should make application directly to the agency that contributed the questioned information. The subject may also direct his challenge to the FBI CJIS Division. The FBI will then forward the challenge to the agency that submitted the data requesting that agency to verify or correct the challenged entry.

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

7.2. How are individuals notified of the procedures for seeking access to or amendment of their information?

In addition to the notice provided in the regulations cited in subsection 7.1 above, notice is provided in the SORNs for the FIRS and the NCIC, which are available on the FBI's Internet website. Federal, State, local, or tribal agencies that contribute information to the NGI and/or the NCIC may have provided notice regarding access to or amendment of their source records.

7.3. If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

N/A

can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

The privacy issue present here would be adequacy of opportunities or procedures[9] whereby individuals might ascertain what information about them is maintained in the NGI and the NCIC and correct any erroneous information. For discussion of the issue of adequate notice, please see subsection 6.4 above. The risk of erroneous information is mitigated because the FBI recognizes it has discretion to correct erroneous information, and indeed the FBI (as well as each agency that contributes information to the NGI and the NIC) has a substantial mission need to ensure the accuracy of information in these systems, and to promptly take appropriate action to correct any erroneous information of which it may become aware. Additionally, this risk is mitigated because the maintenance and dissemination of information in the NGI and NCIC must comply with the provisions of any applicable law, regulation, or policy, including the Privacy Act. This risk is further mitigated to the extent that an agency that contributes information to the NGI and/or NCIC has a process in place for access to or correction of the contributing agency's source records.

No law enforcement action should be taken solely on the basis of RISC submission results because they are not considered positive identification; the law enforcement officer should supplement the candidate information with additional investigatory information before taking a law enforcement action.

Section 8.0 – Technical Access and Security

8.1. Which user group(s) will have access to the system?

User group access to the RISC will be limited to those agency users who have access to information in the NGI and the NCIC. (See sections 4 and 5 above.)

8.2. Will contractors to the Department (DOJ/FBI) have access to the system?

Yes.

8.3. Does the system use "roles" to assign privileges to users of the system?

Yes. Access to the NGI and NCIC is controlled through extensive, long-standing user identification and authentication procedures. The NGI (including the RISC) is not available to users unless there has been an application for, and assignment of, access permission. Each using entity may only access the types of information for the purposes that have been authorized for the entity. Such access is strictly controlled and audited by state agencies and the CJIS Division. There is a separate process for requesting access to RISC. The supervisory authority at each agency with a CJIS WAN connection wishing to participate in RISC must initiate a request for RISC access. For state RISC submissions, the state's central NGI supervisory authority will be the coordination point for determining which state users will be authorized to initiate RISC submissions, the circumstances under which RISC submissions are permissible, and permissible uses of RISC responses. For federal RISC submissions, the federal agency's designated CJIS System Agency will be the coordination point for determining which agency users will be authorized to initiate RISC submissions, the circumstances under which RISC submissions are permissible, and permissible uses of RISC responses.

8.4. What procedures are in place to determine which users may access the system and are they documented?

The applicable agency supervisory authority (CJIS System Officer) or appropriate FBI official must document each request for access permission and reference the statute, regulation, or order that authorizes such access. These procedures have been documented in CJIS security standards and operating policies applicable to all NGI and NCIC users.

8.5. How are the actual assignments of roles and rules verified according to established security and auditing procedures?

The NGI System Design Document includes requirements to maintain chronological transaction audit logs for authorized purposes. Transaction logs are kept for auditing and tracking purposes and to meet recordkeeping and disclosure accounting requirements under the Federal Records Act and the Privacy Act. All users are subject to periodic on-site audits conducted by both a user's own oversight entity and the FBI CJIS Division Audit Unit to assess and evaluate users' compliance with CJIS' technical security policies, regulations, and laws applicable to the criminal identification and criminal history information in NGI, and terms of the applicable user agreements or contracts. Deficiencies identified during audits are reported to the CJIS Division APB's and the Compact Council's Sanctions Committees. Access may be terminated for improper access, use, or dissemination of system records. In addition, each NGI Information System Security Officer (ISSO) is responsible for ensuring that operational security is maintained on a day-to-day basis. Adherence to roles and rules is tested as part of the security certification and accreditation process.

8.6. What auditing measures and technical safeguards are in place to prevent misuse of data?

Please see the discussion in subsection 8.5 above.

8.7. Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

Please see subsection 5.5.

8.8. Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. IAFIS Certification & Accreditation (C&A) under the Federal Information Security Management Act (FISMA) was most recently completed on October 30, 2009. NGI, and RISC, will fall under the IAFIS C&A boundaries. NCIC C&A under FISMA was most recently completed on October 6, 2009.

8.9. Privacy Impact Analysis: Given the access and security controls, what privacy risks were identified and how they were mitigated.

The RISC will be subject to the same extensive security protections, access limitations, and quality control standards in existence for the NGI, thus presenting no new risks in these areas. The October 2009 C&A did not identify any risks in the area of technical access and security. Previously identified risks related to potential misuse of the system, and these risks have been addressed via training, audits, and sanctions. To further mitigate any potential risks in these areas, NGI data and infrastructure (which will encompass the RISC) are maintained within FBI-controlled secure, restricted areas and are accessible only by authorized personnel. Wireless transmissions and mobile devices outside FBI control are subject to the CJIS Security Policy. RISC mobile devices must use the American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST) standards[10] as implemented in the FBI EBTS and be approved by the FBI.

Section 9.0 – Technology

9.1. Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

Yes. NGI system functional and security requirements are pre-established by the FBI prior to the introduction of new technologies. Functional system requirements are derived from end-user needs, applicable laws, and established policy and/or guidelines. Additionally, the NGI development and integration contract includes a series of biometric search analysis studies that will assess biometric technology and provide recommendations for implementation. Mobile devices used for RISC submissions must be approved by the FBI. All mobile devices must meet the current CJIS Security Policy requirements including data encryption and advanced authentication.

9.2. Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

contract. The developer will be required to follow all CJIS Division guidelines, appropriate regulations, and specific statutes. Those agencies and entities with electronic connectivity must comply with, inter alia, requirements contained in the CJIS Division's security standards and operating policies. (See subsection 9.3 below.)

9.3. What design choices were made to enhance privacy?

The NGI Program Office chose to develop a new system by utilizing existing channels and established security measures. With continued input from the CJIS Division APB and participating agencies, the system is designed to comply with the extensive privacy protection built into the existing infrastructure such as established policies, procedures, access controls, and physical security measures that are ensured by audits.

Furthermore, the FBI is developing and implementing the new RISC capabilities only after critical performance parameters have been carefully specified, assessed and confirmed through functional and system requirements analysis and piloting. Effectiveness factors will be developed, monitored, and measured throughout the system life cycle.

Conclusion

The RISC does not constitute a new collection type or collection purpose not encompassed by the NGI or NCIC, nor does it represent any expansion of users authorized to access this information. Instead, the RISC will merely collate a subset of existing NGI identity records to permit employment of specialized biometric-based search techniques in field encounters, rapid searches of the collated information, and rapid responses to authorized users. In addition, the RISC will automatically search RISC submissions against the existing NGI ULF, and search NCIC for any existing NCIC information appropriate for inclusion in RISC responses.

As previously discussed, the RISC does present certain privacy risks. However, these risks can be appropriately mitigated. Mitigation elements include the long-standing technology protections present in the underlying NGI and NCIC systems, the existing eligibility limitations and careful vetting of system users, and the existing access policies, training requirements, and audits. Privacy risks are further mitigated by the responsibility imposed on each user agency to ensure that the collections and uses of fingerprints obtained for RISC submissions are lawful and permissible under the laws and policies of the governmental jurisdiction to which the user agency is subject.

As appropriately mitigated, any additional privacy impact is outweighed by the RISC advantages. These include the added flexibility and simplicity via accommodation of searches using fewer than ten fingerprints, rapid real-time search and response capability in time critical field encounters; enhanced investigative support and crime solving; enhanced accuracy and privacy protection over mere name-based searching, including reduction of the false positives, and greater protection for the public and law enforcement personnel.

Issued by James J. Landon, Chief Privacy and Civil Liberties Officer, Federal Bureau of Investigation

Reviewed by Vance E. Hitch, Chief Information Officer, Department of Justice

Approved by Nancy C. Libin, Chief Privacy and Civil Liberties Officer, Department of Justice
Approved January 18, 2012

Endnotes

[1] NGI will eventually replace the Integrated Automated Fingerprint Identification System (IAFIS) and hold the largest collection of digital representations of fingerprint images and other biometrics. IAFIS is a component of the FBI Privacy Act system of records currently titled the "Fingerprint Identification Records System" (FIRS) (JUSTICE/FBI-009) (64 FR 52343, 52347; 66 FR 33558; 70 FR 7513, 7517; 72 FR 3410). For purposes of this PIA and to minimize confusion, we are referring to the current system as NGI, even though its development will be incremental and currently the fingerprint images are part of IAFIS. Information about IAFIS can be found at http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis, and about NGI at http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi.

[2] In a typical fingerprint analysis, once the system has identified a match, a CJIS fingerprint examiner actually looks at the records to determine if there is, in fact, a match.

[3] The IPS is an NGI component with the capacity for retaining, managing, and searching photographic images associated with NGI records. For additional information, see the NGI/IPS PIA dated June 9, 2008, available on the FBI Internet website.

[4] ULF searches consume significantly more system resources than RISC searches, and ULF search times will vary depending on system loads and priorities.

[5] In November 2007, the FBI CJIS Division began piloting the RISC rapid search capability with selected State and local law enforcement agencies. Over 500,000 requests have been processed since the inception of the RISC pilot with post-processing analysis completed on all responses. This analysis determined there were no (0%) false positives within the top two candidates selected by the system. This same analysis determined 90% of the yellow responses returned included valid identifications.

[6] Both SORNs are available on the FBI's Internet website at http://www.fbi.gov/foia/privacy-act/systems-records.

[7] The FBI is seeking NARA's approval to increase this to 110 years of age.

[8] This telecommunications infrastructure includes the CJIS Wide Area Network (CJIS WAN). The CJIS WAN connects authorized user agencies to the FBI's host computer systems, via a collection of Virtual Private Network (VPN) links and near point-to-point T-1 and higher class data lines connecting the FBI CJIS Data Center in West Virginia to selected points throughout the United States and Canada. This infrastructure includes the International Justice and Public Information Sharing Network (NLets, previously known as the National Law Enforcement Telecommunications System (NLETS)). NLets is a not-for-profit law enforcement communications channel owned and governed by the States and available throughout the United States. This infrastructure includes the respective regional, State, and local networks of the participating agencies.

[9] Applicable opportunities and procedures are discussed in subsections 7.1 and 7.2 above.

[10] The ANSI/NIST standards define the content, format and units of measurements for the exchange of information that may be used in the fingerprint identification of a subject. These standards are intended for use in the interchange between criminal justice administrations or organizations that use an Automated Fingerprint Identification System (AFIS) and to provide a common interface for other AFIS and related systems worldwide.

IAFIS NGI RISC

Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Repository for Individuals of Special Concern (RISC)

Privacy Impact Assessment
Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI)
Repository for Individuals of Special Concern (RISC)

I. Introduction

This Privacy Impact Assessment (PIA) addresses the Repository for Individuals of Special Concern (RISC), an extract of data in the Next Generation Identification (NGI)[1] that is collated for the purposes of providing an enhanced capability to identify persons who present special risks to the public or law enforcement personnel or heightened investigative interest. RISC will facilitate faster and easier searches of NGI by authorized users in field settings.

I.1. Background

In developing the NGI, the FBI sought to identify necessary improvements in its biometric collections. As part of this process, the FBI canvassed the user and law enforcement communities for their input on desired changes, enhancements, and new initiatives for the system. From September 2005 through March 2006, over 190 groups representing 1,000 user agencies were asked for suggestions on upgrades. Multiple users recommended the expansion of existing capabilities or the development of new functionality to support rapid biometric searches with fewer than ten fingerprint images in time-critical situations involving heightened investigative interest or increased risk to the public and/or to law enforcement personnel. After analyzing this input, a task force of the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) suggested the RISC enhancement.

I.2. RISC Enhancement

The RISC will encompass a subset of NGI sensitive but unclassified data, consisting of records of known or appropriately suspected terrorists, wanted persons, registered sexual offenders, and (potentially) other categories of heightened interest warranting more rapid responses to inquiring criminal justice users. (Any additional categories proposed for inclusion, such as missing persons or protection order subjects that have associated biometrics currently in NGI could be considered for RISC. This PIA will be annotated to reflect the addition of any other categories of records.)

The RISC will be queried by fingerprints (10 or fewer) electronically submitted by authorized NGI users, typically by first responder law enforcement officials in the course of their interaction with potential suspects or similar real-time encounters. The fingerprints will be captured by a mobile fingerprint device and transmitted wirelessly to the user agency's existing criminal justice infrastructure, then on to the RISC. The RISC will accommodate so-called "lights-out" processing using fewer than ten fingerprints. Lights-out processing refers to searches that are conducted entirely by computer automation, without any intervening involvement by humans.[2]

The submission will result in an automated search of RISC records and lights-out generation of a response to the requestor's criminal justice infrastructure within ten seconds of the submission. The requestor's criminal justice infrastructure will then forward the response to the requestor's mobile device through its own communication channels. The RISC responses will be either "red," "yellow," "green," or "reject."

Red Response. A red response is a hit, indicating identification of a highly probable candidate in the RISC. However, a red response is not to be considered a positive identification, but rather the 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 ten-print search and/or confirmation of a match by trained fingerprint examiners.) It will be incumbent on the submitting agency to supplement the RISC response with other information to confirm whether or not the candidate returned is indeed the person whose prints were submitted.

A red response will contain the following additional information from NGI: the category of hit (e.g., wanted person, sexual offender registry subject, or known or appropriately suspected terrorist), the identified subject's FBI Number (FNU) and master file name, and if requested by the law enforcement official, any available photos of the subject maintained in the NGI Interstate Photo System (IPS).[3]

Furthermore, for red responses where underlying details of the hit may be important to officer/public safety (e.g., wanted persons or known or appropriately suspected terrorists), the RISC will cascade an automated inquiry of the National Crime Information Center (NCIC) person files using the matched subject's FNU. If matching NCIC data is located, the RISC response will contain pertinent data fields from the relevant NCIC file(s), including NCIC excerpts indicating the nature of any offenses and any applicable warnings or cautions.

Yellow Response. A yellow response is a possible hit, indicating identification of a possible candidate (or candidates) in the RISC but one below the level of confidence established for a highly probable match (red response). The yellow response may thus only be used as an investigative tool providing leads for further investigative inquiries.

Yellow responses may contain the same type of supplemental information as red responses pertinent to the person(s) identified as a possible match (i.e., yellow responses may contain information from NGI regarding the category of the possible hit and underlying details, name and associated system numbers, and available photos). This may, for instance, include photos or other biographic data of possible candidates that could assist the requestor in ascertaining if the candidate is, or is not, a match.

Green Response. A green response indicates no hit (i.e., the search did not locate a viable candidate in the RISC).

Reject Response. The RISC will return a reject response when the quality of the RISC submission is too low to be used for a RISC search.

All red, yellow, and green RISC responses will include a caveat that the response is based solely on a search of the RISC, and that a negative response from the RISC does not preclude the possibility of responsive records in other biometric or name-based repositories. Additionally, RISC users are advised they are prohibited from relying solely on RISC Rapid Search responses as the impetus for any law enforcement action. Instead, search responses serve as potential links between submitted images and true identities that must be considered with the totality of information available to the officer or investigator. This guidance is provided in Memoranda of Understanding (MOUs) between CJIS and RISC users and/or in CJIS system operating policies with which all users are required to comply. In addition, appropriate reminders of this guidance will be included as caveats in all red and yellow RISC responses.

A search against the RISC will cascade a search of the NGI Unsolved Latent File (ULF), relating to 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. Currently NGI ULF searches require separate biometric queries. The cascaded search of the ULF may take considerably more time than the RISC search,[4] and the results will not be returned to the RISC submitting agency. Instead, if a RISC submission 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 submitter may then further develop this lead as it deems appropriate, which may well include contacting and coordinating with the RISC submitting agency.

User agencies will participate in the RISC on a purely voluntary basis. If a user agency opts to submit fingerprints for RISC checks, the agency will need to procure the necessary software, mobile fingerprint capture devices, and infrastructure to provide its law enforcement officers the ability to scan fingerprint images in field settings and transmit these images to the FBI for comparison against the RISC. The information transmitted will be anywhere from two to ten rolled or flat fingerprint images obtained via the mobile fingerprint capture device. The RISC submission will include header information identifying the submitting agency and a unique submission number, but will not include the subject's name or other biographic or event information.

RISC submissions will not be added to or otherwise retained in the NGI identity records. An incoming RISC submission's active presence in the NGI system will be transitory, lasting only for the time needed to complete the automated searching. This will take only seconds for the RISC search itself (including any cascaded NCIC search), plus the additional time required for the slower cascaded search of the ULF.

If a RISC submission results in a ULF hit, NGI will generate a notification to the ULF record submitter advising that a potential match has occurred on their ULF submission and providing the agency identifier and submission number for the RISC submission. NGI will generate and retain chronological transaction audit information for each RISC submission and response. If a RISC submission results in a ULF hit, NGI will generate and retain chronological transaction audit information regarding the ULF hit notice sent to the ULF submitter. Similarly, if the RISC cascades a search to the NCIC, the NCIC will generate and retain chronological transaction audit information regarding the NCIC submission and response.

Section 1.0 – The System and the Information Collected and Stored within the System

1.1 What information is to be collected?

As described above, this initiative does not involve a new collection of information from the persons whose records will be placed in the RISC. The RISC entails a specially collated subset of existing records to permit employment of specialized search techniques, much faster searches of the collated information, and much faster responses to authorized users. The RISC subset will consist of NGI records of known or appropriately suspected terrorists, wanted persons, registered sexual offenders, and other special interest categories warranting more rapid biometric-based responses to inquiring users in time-critical situations involving heightened investigative interest or increased risk to the public and/or to law enforcement personnel.

The fingerprint images used to initiate a RISC check typically will be newly collected in field encounters by law enforcement officers for the user agency's own purposes under the user agency's own mission authorities. As with all biometric submissions to CJIS, the user agency will have the sole responsibility for determining whether to collect these fingerprints and must ensure any such collections and uses are lawful and permissible. Similarly, whether or not the collected fingerprints will be retained by the user agency (or by other instrumentality of the user agency's governmental jurisdiction), will be solely determined by the user agency pursuant to its laws and policies.

CJIS is maintaining fingerprint images submitted during the prototype and rollout phase of RISC. Per the MOUs, at the conclusion of the prototyping phase, CJIS will delete or destroy all fingerprint images received

from state identification bureaus. Once fully operational, RISC fingerprint submissions will not be added to or otherwise retained in the NGI records.

Transaction logs are created for all incoming and outgoing RISC transactions. The incoming submission logs contain the transaction data, the name of the officer capturing the fingerprints, the make, model and serial number of the image capture equipment, the request for the rap sheet or photograph when indicated, and the name of the repository to be searched. The outgoing transactions return the aforementioned incoming transaction data to the requester, as well as the FBI number, name, and place of birth when candidates result from the search.

1.2. From whom is the information collected?

Information used to populate the RISC, or that will be accessed via the RISC functionalities, will be obtained from existing NGI and NCIC records relating to those categories of persons identified in subsection 1.1 above. This information will have been collected and submitted to the FBI by federal, state, local, tribal, and some foreign agencies and instrumentalities incident to their lawful mission. Most of the biometric information will have been obtained directly from the subject by the submitting agencies, but some may have been obtained indirectly (such as latent fingerprints obtained from crime scenes). Related biographic and event information may either have been obtained directly from the subject by the submitting agencies, or obtained by the submitting agencies from other sources in the course of investigations or other authorized activities.

The biometric images used to initiate a RISC check typically will be newly collected from persons who are the subjects of field encounters by officers and employees of user agencies incident to authorized activities of these agencies. The user agencies may then opt to forward these biometrics to the NGI for RISC checks. In almost all such cases the biometrics will be obtained directly from and with the knowledge of the subject. The collections will be lawful and permissible under applicable laws and policies of the governmental jurisdiction to which the user agency is subject.

Section 2.0 – The Purpose of the System and the Information Collected and Stored within the System

2.1. Why is the information being collected?

The RISC will collate a subset of existing NGI identity records to permit employment of specialized biometric-based search techniques, much faster searches of the collated information, and much faster responses to authorized users in time-critical situations. The RISC will permit rapid, practicable, biometric-based searches in field settings. The resulting benefits will include greater protection for the public and law enforcement personnel, enhanced investigative support, and reduced impact of law enforcement activities on innocent persons with biographic similarities to persons of investigative interest. Before the RISC, biometric-based searches of NGI required the submission of a full set of ten prints, which as a practical matter could only be captured at the user agency's office, to which the subject would have to be transported following arrest or detention. Identity checks in field settings were thus limited to biographic-based checks (such as name and date of birth) which do not uniquely identify a person and could be unreliable due to misinformation provided by the subject and/or misassociation with persons with biographic similarities.

Transaction logs are kept for auditing and tracking purposes and to meet recordkeeping and disclosure accounting requirements under the Federal Records Act and the Privacy Act. There will be no new use of audit log information pursuant to the RISC initiative.

Fingerprint images are being collected during the prototype phase to allow FBI to conduct reviews of all transactions by human fingerprint specialists to assess the accuracy of responses (see Section 2.3).

2.2. What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

The statutory authority for this initiative is 28 U.S.C. §§ 533 and 534. Supplemental regulatory authorities include 28 C.F.R. § 0.85, part 20, and 50.12. The Attorney General has delegated the responsibilities set forth in 28 U.S.C. § 534 to the Director of the FBI, and the Director has further delegated them to the FBI CJIS Division. Additional authorities include 42 U.S.C. § 3771; 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; EO 13311 (amended by EO 13388); EO 13388.

The Federal Records Act (FRA), codified at 44 U.S.C. § 3301 et seq., provides another general statutory basis for the FBI to retain and preserve materials submitted for FBI checks and/or obtained by the FBI in the course of authorized investigative activities, in order to ensure adequate and proper documentation of FBI activities.

Currently, an MOU is executed between the FBI/CJIS and each user agency during the RISC development, testing, and roll-out. The MOU details the processes, conditions, and limitations regarding the transmittal, receipt, storage, use, and dissemination of information relating to this initiative. Eventually, RISC coverage will be incorporated into standing CJIS security standards and operating policies applicable to all CJIS users.

2.3. Privacy Impact Analysis: Given the amount and type of data collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

Privacy risks for the RISC arise from any potential vulnerabilities presented by the new RISC processes. Several such risks have been identified and are addressed below.

There would be a new risk if the RISC method(s) for submitting fingerprints were less effective in accurately identifying responsive records, resulting in an unacceptable percentage of misidentifications. A misidentification could result in a false positive or false negative. A false positive mistakenly declares a probable or possible match; any such erroneous information could be returned to the requestor, thereby possibly 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 requestor, thereby possibly thwarting investigative efforts and posing a safety hazard to the unwarned requestor and/or to the public. Recognizing this risk, the FBI is taking great care in calibrating and adjusting the red-yellow-green thresholds to ensure accuracy while providing enough actionable decisions (red or green) to be beneficial to the officer in the field.[5] For the final NGI RISC solution, the NGI System Requirements Document establishes the following criterion: "NGI shall return the correct candidate a minimum of 98% of the time, when it exists in the RISC repository, as a result of a fingerprint feature search in support of RISC rapid searches." CJIS will continue to monitor the accuracy of RISC searches via periodic sampling and audits throughout the system life cycle.

Furthermore, a RISC search submitted from a mobile device is not designed or expected to take the place of customary booking procedures that utilize tenprint submissions. The FBI will emphasize via piloting MOUs and revisions to security standards and operating policies applicable to all system users that RISC responses are not to be considered "positive" identifications and must be used only as investigative aids together with other investigative processes and information. Moreover, as a counterbalancing benefit, a RISC search will make available biometric-based searches in time-sensitive situations where previously only name-based searches were viable. These biometric-based checks can provide more accuracy than name-based checks alone, reducing the number of erroneous identifications in these situations.

Fingerprint submissions to the RISC may involve fewer than ten fingerprints, and may include "flat" prints

rather than "rolled" prints. Regarding identification based on a lesser number of fingerprints, the FBI considers that the system's fingerprint technology and technical capacity has sufficiently progressed to permit extremely accurate association with an existing record based on comparison with an existing ten-print set associated with the record. Similarly, based on recent post-processing analysis of over 500,000 submissions, the FBI has determined flat prints provide sufficient biometric features to permit the identification of a highly probable candidate in the RISC. Moreover, live scanning and scanning fewer than ten fingers contributes to the portability of the capture devices. This facilitates the use of the devices in field settings to obtain the accuracy advantages of biometric-based searches in these settings.

There is a risk that fully automated lights-out responses to RISC submissions will not be as accurate as responses that have been confirmed by fingerprint comparisons conducted by humans, thus resulting in an unacceptable percentage of misidentifications. In an attempt to mitigate this risk, during the RISC rollout, CJIS is conducting follow up review of all transactions by qualified fingerprint staff. These reviews are being documented, and any issues are recorded and reported to ensure accuracy of the fingerprint comparisons. The results of these reviews are being studied, and current post-processing analysis has not identified any "false positive" errors in automated RISC responses to submissions from portable capture devices.

There could be a risk that the process for automatically using an incoming RISC biometric query as the basis to generate a text-based query of NCIC might not be sufficiently reliable to produce an appropriate NCIC query, thereby either missing related records in NCIC that should have been returned or returning another subject's NCIC records. To mitigate this risk, all cascaded NCIC searches are accomplished by using the FNU from the biometric record, so that any NCIC responses will be linked by a unique identifier established from positive biometric identification. Although there remains the conceivable risk of erroneous FNU linkage resulting from human error, system failure, or data corruption, this risk is considered extremely small because of CJIS system maintenance standards and audits conducted by State agencies and the CJIS Division. This risk is mitigated by the caveat provided with all RISC responses notifying the user that the RISC search is only a search of the RISC repository and does not preclude a record from existing in other biometric or name based repositories. Additionally, this risk is further mitigated by guidance currently in MOUs and to be incorporated into standing CJIS security standards and operating policies emphasizing that RISC users should not rely on RISC results alone prior to taking any adverse action against a person.

Similarly, there could be a risk that the process for automatically using an incoming RISC biometric query as the basis to generate a biometric-based search of the ULF might not be sufficiently reliable to produce an accurate result, thereby either missing a related ULF record (false negative) or erroneously returning an unrelated ULF record (false positive). The risk of false negatives is not significant because RISC-based ULF searches provide a new capability but do not supplant any existing capability. If a RISC search returns a false negative, the impact (failure to make the ULF connection based on a field check) will be no different from the current situation (inability to make a ULF field check), and the ULF connection can be made later via any separate opportunities for direct searches of the ULF that might occur. The risk of false positives is mitigated because the ULF results are not returned to the RISC submitter in the field (where erroneous "hits" might subject the affected individuals to unwarranted law enforcement responses during the real-time field encounters). Instead, the ULF results are returned to the ULF submitter as potential matches, to be used in the fullness of time as possible leads for further investigative activity (to include subsequent expert examination to positively confirm or rule out any matches).

An additional privacy vulnerability is present to the extent that the RISC enhanced search and response capabilities provide an increased ability to locate information about a specific person that might not otherwise be discovered as quickly or as efficiently, or might never be discovered at all. Although information in NGI and NCIC will have been lawfully acquired and accessible to authorized NGI and NCIC users, currently that information may be more functionally obscure as a result of users having to separately check multiple systems or encountering longer response times. However, this risk is mitigated by the advantages of being able to move

quickly and accurately to locate responsive information about a specific person. This capability permits more complete and timely investigative analysis, including more effective and efficient identification of perpetrators and persons who may present increased threats to the safety of the public and law enforcement personnel. The privacy risk is also mitigated by facilitating a more rapid means to eliminate misidentifications and/or rule out concerns that could adversely impact innocent persons.

Another privacy risk could be the ingestion of records that do not belong in the RISC repository. The possibility of the occurrence of this risk is mitigated by CJIS procedures that ensure that fingerprints of wanted, KSTs, and sex offenders are appropriately flagged as they are entered into IAFIS. RISC extracts records based on those flags.

Furthermore, the FBI is developing and implementing the new RISC capabilities only after critical performance parameters have been carefully specified, assessed and confirmed through functional and system requirements analysis and piloting. Effectiveness factors will be developed, monitored, and measured throughout the system life cycle.

Section 3.0 – Uses of the System and the Information

3.1. Describe all uses of the information.

RISC searches will be available only to users authorized to initiate searches of NGI and NCIC for authorized law enforcement or national security purposes. Routine uses for information in NGI are currently promulgated in the System of Records Notice (SORN) for the FBI Fingerprint Identification Records System (FIRS), and routine uses for information in the NCIC are promulgated in the NCIC's SORN.[6] In addition to routine use disclosures, this information may be disclosed under other circumstances authorized by the Privacy Act, including disclosures to those Department of Justice (DOJ) personnel who need the information in the performance of their duties.

The results of RISC searches will be used by law enforcement officers as leads to determine the identity and relevant history of the subject and take appropriate investigatory action, and, if necessary, precautions for his or her own safety.

As discussed in section I above, RISC submissions will cascade searches against the latent fingerprints present in the NGI ULF. If a RISC submission results in a ULF hit, NGI will generate a notification to the ULF record submitter advising that a potential match has occurred on their ULF submission and providing the agency identifier and submission number for the RISC submission. The ULF record submitter may then further develop this lead as it deems appropriate to resolve the pending investigation relating to the latent fingerprint.

The transaction logs are used by the CJIS Audit Unit to conduct recurrent audits to ensure the proper access, use, and dissemination of IAFIS/NGI records.

3.2. Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

No. The RISC process (and any cascaded searching of the ULF and NCIC) only involve biometric-based searches to identify pertinent information that may relate to the specific subjects of the RISC checks.

3.3. How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

The NGI and NCIC encompass substantial processes to ensure accuracy of information. The RISC will

comprise a subset of information existing in the parent NGI system and thereby subject to the system's existing data quality standards and operating policies. Under these existing requirements, NGI and NCIC users are responsible for ensuring that accurate and complete biographical information is included in NGI and NCIC submissions and that any associated biometrics meet CJIS quality standards. The CJIS Audit Unit regularly checks representative samples of NGI and NCIC submissions for compliance. In addition, the mobile devices used for RISC submissions must be approved by the FBI and comply with the FBI Electronic Biometric Transmission Specification (EBTS), which defines requirements to which agencies must adhere when electronically communicating with CJIS, helping to ensure the accuracy, image quality, and interoperability of RISC submissions. (See subsection 9.1 below.)

3.4. What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

The National Archives and Records Administration (NARA) has approved the destruction of fingerprint cards and corresponding indices when criminal subjects attain 99 years of age,[7] or seven years after notification of death. NARA has determined automated FBI criminal identification records (rap sheets) and NGI and NCIC transaction logs are to be permanently retained. Biometrics and associated biographic information may be removed from the NGI earlier than the standard NARA retention period pursuant to a request by the submitting agency or the order of a court of competent jurisdiction.

RISC submissions will not be added to or otherwise retained in NGI identity records. An incoming RISC submission's active presence in the NGI system will be transitory, lasting only for the seconds needed for the RISC search itself (including any cascaded NCIC search), plus the additional time required for the slower cascaded search of the ULF. Chronological records of RISC and NCIC submissions and responses (including any ULF hit notices) will be permanently retained in the respective NGI and NCIC transaction logs. (See subsections I.2 and 1.1 above.)

3.5. Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Please see the discussion in subsection 2.3 above and section 8 below.

Section 4.0 – Internal Sharing and Disclosure of Information within the System

4.1. With which internal components of DOJ is the information shared?

Components of DOJ may make RISC submissions and receive candidate information in the same manner as other state, local, and federal law enforcement partners. This will primarily encompass the following DOJ components whose missions typically involve interactions in field settings with persons associated with criminal activity or otherwise having a lawful investigative or national security interest: the FBI, the Drug Enforcement Administration (DEA), the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the Federal Bureau of Prisons (BOP), the United States National Central Bureau INTERPOL, and the United States Marshals Service (USMS). In addition, any DOJ component that has previously submitted a latent fingerprint to the NGI ULF file will be notified if a RISC submission hits on that latent fingerprint.

4.2. For each recipient component or office, what information is shared and for what purpose?

The results of RISC searches will primarily be given to a submitting component's on-scene employees in real time whenever the subject of the RISC submission may be a wanted person, registered sexual offender, known or appropriately suspected terrorist, or other person of heightened investigative interest or who may present increased risk to the public and/or to law enforcement personnel. In addition, if a RISC submission results in a

ULF hit on a latent fingerprint previously submitted by a DOJ component, the submitting component will be notified of the potential match for use as a lead in furthering the investigation involving the latent fingerprint. Authorities for these disclosures include those cited in subsection 2.2 above.

For additional discussion of the contents of RISC responses and the purposes underlying the RISC, please refer to section I, section 2, and subsection 3.1. above.

4.3. How is the information transmitted or disclosed?

The RISC will typically be queried on a case-by-case basis by authorized NGI users incident to real-time encounters in field settings, when two to ten fingerprints may be captured by an FBI-approved mobile fingerprint device and transmitted wirelessly to the user's headquarters and then on to the RISC using existing NGI communications infrastructure.[8] The results of a RISC search will be returned to the submitting headquarters via existing NGI communications infrastructure and may then be wirelessly transmitted back to the field user. If a RISC submission results in a ULF hit on a previously submitted latent fingerprint, the latent-submitting component will be notified of the potential match via existing NGI communications infrastructure.

4.4. Privacy Impact Analysis: Considering the extent of internal information sharing, discuss what privacy risks were identified and how they were mitigated.

Information is disclosed only to DOJ users who have been given authorized access to the information in NGI and the NCIC in accordance with all applicable laws, regulations, SORNs, and long-standing CJIS security standards and operating policies applicable to all system users.

There could be a risk if the technology used for RISC submissions were unreliable, insecure, or incompatible with the RISC processes. To mitigate this risk, mobile devices used for RISC submissions must be approved by the FBI. Additionally, all mobile devices must meet the current CJIS Security Policy requirements including data encryption and advanced authentication. The CJIS Security Policy also contains standards for wireless transmissions that require establishment of usage restrictions and implementation guidance for wireless technologies and authorization, monitoring, and controlling of wireless access to information systems. Once the RISC wireless transmissions reach the submitting agency's headquarters, onward routing of the submission to the RISC will be via existing NGI communications infrastructure incorporating extensive security safeguards.

Please see subsections 2.3 above and 5.4, 5.5, and 5.6 below.

Section 5.0 – External Sharing and Disclosure

5.1. With which external (non-DOJ) recipient(s) is the information shared?

Federal, state, local, tribal, foreign, or international governmental agencies which are authorized access to the underlying information in the NGI and the NCIC and which requires the information in the furtherance of its lawful mission may make RISC submissions and receive candidate information. This will primarily encompass those agencies whose missions involve interactions in field settings with persons associated with criminal activity or related to criminal justice or authorized national security investigations. In addition, any NGI user that has previously submitted a latent fingerprint to the NGI ULF file will be notified if a RISC submission hits on that latent fingerprint.

5.2. What information is shared and for what purpose?

The results of RISC searches will primarily be given to authorized NGI and NCIC users in order to alert a submitting agency's on-scene employees in real time whenever the subject of the RISC submission may be a

wanted person, registered sexual offender, known or appropriately suspected terrorist, or other person of heightened investigative interest or who may present increased risk to the public and/or to law enforcement personnel. In addition, if a RISC submission results in a ULF hit on a latent fingerprint previously submitted by a law enforcement agency, the submitting agency will be notified of the potential match for use as a lead in furthering the investigation involving the latent fingerprint. Authorities for these disclosures include those cited in subsection 2.2 above.

5.3. How is the information transmitted or disclosed?

The transmission of information is the same as for internal sharing, described in 4.3.

5.4. Are there any agreements concerning the security and privacy of the data once it is shared?

Title 28 U.S.C. § 534 provides that the dissemination of information under its authority is subject to cancellation if shared information is disclosed outside the receiving agency or related agencies. Title 28 C.F.R. § 20.33 provides supplemental guidance regarding the dissemination of criminal history record information, including identification of authorized recipients and possible sanctions for unauthorized disclosures. These restrictions are in turn reflected in longstanding and extensive NGI and NCIC security standards and operating policies applicable to all system users.

In addition, the FBI has entered into RISC-specific MOUs with all participating agencies and similar provisions will eventually be added to CJIS operating policies. These MOUs generally include provisions emphasizing that the RISC searches will be limited to authorized agencies for authorized purposes and that all CJIS rules regarding access to and use of CJIS information apply. Eventually, these provisions will be incorporated into standing CJIS security standards and operating policies applicable to all CJIS users. All authorized NGI users interfacing with RISC will be required to adhere to these same CJIS rules.

Pursuant to the RISC MOUs and/or upcoming CJIS operating polices, the individual federal and state authorities will establish how RISC responses will be disseminated and maintained. For instance, a state may determine that only red and green responses will be forwarded to on-scene users, or before forwarding RISC responses to on-scene users a State may replace the RISC's red-yellow-green terminology with some alternative terminology preferred by the State (such as probable hit-possible hit-no hit). As another example, one state may decide that RISC responses will not be retained in the State records about the subject, whereas another state may decide that RISC responses will be retained in the state records about the subject.

5.5. What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

Pursuant to longstanding NGI and NCIC security standards and operating policies applicable to all system users, CJIS Systems Officers at the all government levels are responsible for the role-based training, testing, and proficiency affirmation of authorized NGI and NCIC users within their respective organization. All users must be trained within six months of employment and biennially retested thereafter. When implemented, RISC processes will be incorporated as part of this training. The RISC Program Office provides training to all participating agencies regarding RISC capabilities. The participating agencies are responsible for ensuring training on the use of their wireless devices and the appropriate use of RISC, including the fact that RISC responses do not provide the sole justification for law enforcement action.

5.6. Are there any provisions in place for auditing the recipients' use of the information?

Yes. Please see subsections 8.5 and 8.6 below.

5.7. Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and how were they mitigated?

Information is disclosed only to agency users who have been authorized access to the information in NGI and the NCIC in accordance with all applicable laws, regulations, SORNs, and long-standing CJIS security standards and operating policies applicable to all system users.

There would be a risk if the technology used for RISC submissions were unreliable, insecure, or incompatible with the RISC processes. Mitigation of this risk is discussed in subsection 4.4 above.

Please see subsections 2.3, 5.4, 5.5, and 5.6 above.

Section 6.0 – Notice

6.1. Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

The user agencies that contribute the underlying information to the NGI and NCIC likely do not provide any sort of Privacy Act Statements or similar actual notice to the individuals from whom or about whom the information pertains. This is because non-federal contributors are not subject to the Privacy Act, federal contributors are usually exempted from the Privacy Act's individual collection notice provisions in connection with criminal law enforcement activities, and/or provision of individual notice incident to criminal law enforcement activities is typically impracticable.

General notice regarding the collection of information in the NGI and NCIC has been provided to the public at large via the FIRS and NCIC SORNs. RISC is a subset of NGI, and FBI has provided notice under the system of records notice entitled the "Fingerprint Identification Records System" (FIRS) (JUSTICE/FBI-009) (64 FR 52343, 52347; 66 FR 33558; 70 FR 7513, 7517; 72 FR 3410).

The publication of this PIA will provide general advance notice to the public for all RISC-related collections that will occur subsequent to the publication.

Additional notice might be provided by the federal, state, local, or tribal agency which contributes the underlying NGI and NCIC information and/or which conducts the RISC check.

Even absent any formal notice, for the most part the information in the RISC subset will be based on one or more instances of direct criminal justice processing of the individual (such as "booking") of which the individual will be specifically aware. Similarly, the fingerprints in a RISC submission will have been taken incident to direct involvement with law enforcement in a field encounter of which the individual will be specifically aware their fingerprints are being taken. It is the responsibility of the submitting agency to inform the subject, based on standard operating procedures and appropriate use guidance, of the reason for fingerprint collection. In some situations, such as the conduct of criminal investigations or issuance of arrest warrants, the affected individuals may not always be specifically aware that personal information is being collected and disseminated; however, individuals planning or engaging in criminal activities may reasonably be charged with constructive knowledge that law enforcement will zealously seek to collect and lawfully disseminate all relevant information to identify them and to deter or prevent them from committing crimes.

6.2. Do individuals have an opportunity and/or right to decline to provide information?

Because the information in the RISC subset is collected in connection with law enforcement investigations and/or processing, individuals generally do not have the right or opportunity to object to the collection of this information by the source agencies, nor to the forwarding of the collected information for retention in the NGI and/or the NCIC, nor to the collation of the RISC subset from information in the NGI.

Whether or not individuals will have the right or opportunity to object to the collection of the fingerprints used to initiate a RISC check, and the consequences for objecting, will depend on the location and circumstances of the particular field encounter from which the fingerprints were obtained. All collections must be lawfully obtained under the laws, regulations, and policies to which the agency that obtained the fingerprints may be subject. In many instances the fingerprints for RISC checks may be collected in connection with law enforcement investigations and/or processing in which the individuals generally may not be accorded the right or opportunity to object to the collection. However, in other instances a submitting agency may be obligated under its governing laws, regulations, and/or policies to accord an individual the right or opportunity to object to the collection; personnel of an encountering agency may, in their discretion, voluntarily elect to ask an individual to consent to the collection. In some situations where an individual declines to consent to collection, the encountering agency may nonetheless be entitled to proceed with nonconsensual collection based on alternative authority. In other situations, however, an individual's failure to consent may be controlling, and the encountering agency will have to forego the collection and resolve the encounter without the benefit of a RISC check. Even where an individual is able to successfully decline to be subject to a RISC check, the consequences will vary. In some circumstances a RISC check would not have affected the eventual outcome of an encounter, so the declination will have no consequences to the individual. In other circumstances the results of the RISC check could have altered the outcome of an encounter. This might result in an individual's avoiding further law enforcement interest if the encountering agency were aware of derogatory RISC information (e.g., a "red" or "hit" response), but it could result in an individual's being subjected to prolonged law enforcement interest that might have been avoided if the encountering agency were aware of a non-derogatory RISC response (e.g., a "green" or "no-hit" response).

6.3. Do individuals have an opportunity to consent to particular uses of the information? If such an opportunity exists, what is the procedure by which an individual would provide such consent?

For the same reasons discussed in subsections 6.1 and 6.2 above, individuals generally do not have the opportunity and/or right to consent to particular uses of the information in the RISC subset, since it is obtained from criminal justice subjects incident to criminal justice processes.

To the extent that an individual may have the option to successfully decline to submit to a RISC check as discussed in subsection 6.2 above, the individual would thereby have the opportunity to decline consent and thereby preclude such a use of his/her fingerprints.

6.4. Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The privacy issue present here would be adequacy of notice to affected individuals about how information about them is being collected, maintained, and used, and adequacy of opportunity for the individuals to effectively object to such collection, maintenance, and/or uses. These risks are mitigated by the general notice to the public at large via the FIRS and NCIC SORNs and by the publication of this PIA. Any such collection, maintenance, and/or uses must comply with the provisions of any applicable law, regulation, or policy, including the Privacy Act. Privacy risks are further mitigated to the extent that collecting agencies in some jurisdictions may in certain instances provide actual notice and/or the opportunity to decline to submit to RISC checks. Although availability of such further mitigation will vary depending on the jurisdiction involved, the differences represent an appropriate deference to the principles of federalism.

Section 7.0 – Individual Access and Redress

7.1. What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Pursuant to subsection (j)(2) of the Privacy Act, RISC-related information is exempt from the individual access, accounting and amendment provisions of the Act due to the law enforcement nature of the information. As such, 28 C.F.R. § 16.30-16.34 and 20.34 provide the only means for access and amendment of criminal history records. Under these regulations, a subject of an FBI identification record may obtain a copy of his or her own record for review and correction. If after reviewing his identification record the subject thereof believes that it is incorrect or incomplete in any respect and wishes changes, corrections, or updating, he should make application directly to the agency that contributed the questioned information. The subject may also direct his challenge to the FBI CJIS Division. The FBI will then forward the challenge to the agency that submitted the data requesting that agency to verify or correct the challenged entry.

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

7.2. How are individuals notified of the procedures for seeking access to or amendment of their information?

In addition to the notice provided in the regulations cited in subsection 7.1 above, notice is provided in the SORNs for the FIRS and the NCIC, which are available on the FBI's Internet website. Federal, State, local, or tribal agencies that contribute information to the NGI and/or the NCIC may have provided notice regarding access to or amendment of their source records.

7.3. If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

N/A.

7.4. Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

The privacy issue present here would be adequacy of opportunities or procedures[9] whereby individuals might ascertain what information about them is maintained in the NGI and the NCIC and correct any erroneous information. For discussion of the issue of adequate notice, please see subsection 6.4 above. The risk of erroneous information is mitigated because the FBI recognizes it has discretion to correct erroneous information, and indeed the FBI (as well as each agency that contributes information to the NGI and the NIC) has a substantial mission need to ensure the accuracy of information in these systems, and to promptly take appropriate action to correct any erroneous information of which it may become aware. Additionally, this risk is mitigated because the maintenance and dissemination of information in the NGI and NCIC must comply with the provisions of any applicable law, regulation, or policy, including the Privacy Act. This risk is further mitigated to the extent that an agency that contributes information to the NGI and/or NCIC has a process in place for access to or correction of the contributing agency's source records.

No law enforcement action should be taken solely on the basis of RISC submission results because they are not considered positive identification; the law enforcement officer should supplement the candidate information with additional investigatory information before taking a law enforcement action.

Section 8.0 – Technical Access and Security

8.1. Which user group(s) will have access to the system?

User group access to the RISC will be limited to those agency users who have access to information in the NGI and the NCIC. (See sections 4 and 5 above.)

8.2. Will contractors to the Department (DOJ/FBI) have access to the system?

Yes.

8.3. Does the system use "roles" to assign privileges to users of the system?

Yes. Access to the NGI and NCIC is controlled through extensive, long-standing user identification and authentication procedures. The NGI (including the RISC) is not available to users unless there has been an application for, and assignment of, access permission. Each using entity may only access the types of information for the purposes that have been authorized for the entity. Such access is strictly controlled and audited by state agencies and the CJIS Division. There is a separate process for requesting access to RISC. The supervisory authority at each agency with a CJIS WAN connection wishing to participate in RISC must initiate a request for RISC access. For state RISC submissions, the state's central NGI supervisory authority will be the coordination point for determining which state users will be authorized to initiate RISC submissions, the circumstances under which RISC submissions are permissible, and permissible uses of RISC responses. For federal RISC submissions, the federal agency's designated CJIS System Agency will be the coordination point for determining which agency users will be authorized to initiate RISC submissions, the circumstances under which RISC submissions are permissible, and permissible uses of RISC responses.

8.4. What procedures are in place to determine which users may access the system and are they documented?

The applicable agency supervisory authority (CJIS System Officer) or appropriate FBI official must document each request for access permission and reference the statute, regulation, or order that authorizes such access. These procedures have been documented in CJIS security standards and operating policies applicable to all NGI and NCIC users.

8.5. How are the actual assignments of roles and rules verified according to established security and auditing procedures?

The NGI System Design Document includes requirements to maintain chronological transaction audit logs for authorized purposes. Transaction logs are kept for auditing and tracking purposes and to meet recordkeeping and disclosure accounting requirements under the Federal Records Act and the Privacy Act. All users are subject to periodic on-site audits conducted by both a user's own oversight entity and the FBI CJIS Division Audit Unit to assess and evaluate users' compliance with CJIS' technical security policies, regulations, and laws applicable to the criminal identification and criminal history information in NGI, and terms of the applicable user agreements or contracts. Deficiencies identified during audits are reported to the CJIS Division APB's and the Compact Council's Sanctions Committees. Access may be terminated for improper access, use, or dissemination of system records. In addition, each NGI Information System Security Officer (ISSO) is responsible for ensuring that operational security is maintained on a day-to-day basis. Adherence to roles and

rules is tested as part of the security certification and accreditation process.

8.6. What auditing measures and technical safeguards are in place to prevent misuse of data?

Please see the discussion in subsection 8.5 above.

8.7. Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

Please see subsection 5.5.

8.8. Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. IAFIS Certification & Accreditation (C&A) under the Federal Information Security Management Act (FISMA) was most recently completed on October 30, 2009. NGI, and RISC, will fall under the IAFIS C&A boundaries. NCIC C&A under FISMA was most recently completed on October 6, 2009.

8.9. Privacy Impact Analysis: Given the access and security controls, what privacy risks were identified and how they were mitigated.

The RISC will be subject to the same extensive security protections, access limitations, and quality control standards in existence for the NGI, thus presenting no new risks in these areas. The October 2009 C&A did not identify any risks in the area of technical access and security. Previously identified risks related to potential misuse of the system, and these risks have been addressed via training, audits, and sanctions. To further mitigate any potential risks in these areas, NGI data and infrastructure (which will encompass the RISC) are maintained within FBI-controlled secure, restricted areas and are accessible only by authorized personnel. Wireless transmissions and mobile devices outside FBI control are subject to the CJIS Security Policy. RISC mobile devices must use the American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST) standards[10] as implemented in the FBI EBTS and be approved by the FBI.

Section 9.0 – Technology

9.1. Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

Yes. NGI system functional and security requirements are pre-established by the FBI prior to the introduction of new technologies. Functional system requirements are derived from end-user needs, applicable laws, and established policy and/or guidelines. Additionally, the NGI development and integration contract includes a series of biometric search analysis studies that will assess biometric technology and provide recommendations for implementation. Mobile devices used for RISC submissions must be approved by the FBI. All mobile devices must meet the current CJIS Security Policy requirements including data encryption and advanced authentication.

9.2. Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Data integrity, privacy, and security will remain a significant part of the enhanced system and the NGI contract. The developer will be required to follow all CJIS Division guidelines, appropriate regulations, and specific statutes. Those agencies and entities with electronic connectivity must comply with, inter alia, requirements

contained in the CJIS Division's security standards and operating policies. (See subsection 9.3 below.)

9.3. What design choices were made to enhance privacy?

The NGI Program Office chose to develop a new system by utilizing existing channels and established security measures. With continued input from the CJIS Division APB and participating agencies, the system is designed to comply with the extensive privacy protection built into the existing infrastructure such as established policies, procedures, access controls, and physical security measures that are ensured by audits.

Furthermore, the FBI is developing and implementing the new RISC capabilities only after critical performance parameters have been carefully specified, assessed and confirmed through functional and system requirements analysis and piloting. Effectiveness factors will be developed, monitored, and measured throughout the system life cycle.

Conclusion

The RISC does not constitute a new collection type or collection purpose not encompassed by the NGI or NCIC, nor does it represent any expansion of users authorized to access this information. Instead, the RISC will merely collate a subset of existing NGI identity records to permit employment of specialized biometric-based search techniques in field encounters, rapid searches of the collated information, and rapid responses to authorized users. In addition, the RISC will automatically search RISC submissions against the existing NGI ULF, and search NCIC for any existing NCIC information appropriate for inclusion in RISC responses.

As previously discussed, the RISC does present certain privacy risks. However, these risks can be appropriately mitigated. Mitigation elements include the long-standing technology protections present in the underlying NGI and NCIC systems, the existing eligibility limitations and careful vetting of system users, and the existing access policies, training requirements, and audits. Privacy risks are further mitigated by the responsibility imposed on each user agency to ensure that the collections and uses of fingerprints obtained for RISC submissions are lawful and permissible under the laws and policies of the governmental jurisdiction to which the user agency is subject.

As appropriately mitigated, any additional privacy impact is outweighed by the RISC advantages. These include the added flexibility and simplicity via accommodation of searches using fewer than ten fingerprints, rapid real-time search and response capability in time critical field encounters; enhanced investigative support and crime solving; enhanced accuracy and privacy protection over mere name-based searching, including reduction of the false positives; and greater protection for the public and law enforcement personnel.

Issued by James J. Landon, Chief Privacy and Civil Liberties Officer, Federal Bureau of Investigation

Reviewed by Vance E. Hitch, Chief Information Officer, Department of Justice

Approved by Nancy C. Libin, Chief Privacy and Civil Liberties Officer, Department of Justice
Approved January 18, 2012

Endnotes

[1] NGI will eventually replace the Integrated Automated Fingerprint Identification System (IAFIS) and hold the largest collection of digital representations of fingerprint images and other biometrics. IAFIS is a component of the FBI Privacy Act system of records currently titled the "Fingerprint Identification Records System" (FIRS) (JUSTICE/FBI-009) (64 FR 52343, 52347; 66 FR 33558; 70 FR 7513, 7517; 72 FR 3410. For purposes of this PIA and to minimize confusion, we are referring to the current system as NGI, even though its development will

be incremental and currently the fingerprint images are part of IAFIS. Information about IAFIS can be found at http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis, and about NGI at http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi.

[2] In a typical fingerprint analysis, once the system has identified a match, a CJIS fingerprint examiner actually looks at the records to determine if there is, in fact, a match.

[3] The IPS is an NGI component with the capacity for retaining, managing, and searching photographic images associated with NGI records. For additional information, see the NGI/IPS PIA dated June 9, 2008, available on the FBI Internet website.

[4] ULF searches consume significantly more system resources than RISC searches, and ULF search times will vary depending on system loads and priorities.

[5] In November 2007, the FBI CJIS Division began piloting the RISC rapid search capability with selected State and local law enforcement agencies. Over 500,000 requests have been processed since the inception of the RISC pilot with post-processing analysis completed on all responses. This analysis determined there were no (0%) false positives within the top two candidates selected by the system. This same analysis determined 90% of the yellow responses returned included valid identifications.

[6] Both SORNs are available on the FBI's Internet website at http://www.fbi.gov/foia/privacy-act/systems-records.

[7] The FBI is seeking NARA's approval to increase this to 110 years of age.

[8] This telecommunications infrastructure includes the CJIS Wide Area Network (CJIS WAN). The CJIS WAN connects authorized user agencies to the FBI's host computer systems, via a collection of Virtual Private Network (VPN) links and near point-to-point T-1 and higher class data lines connecting the FBI CJIS Data Center in West Virginia to selected points throughout the United States and Canada. This infrastructure includes the International Justice and Public Information Sharing Network (NLets, previously known as the National Law Enforcement Telecommunications System (NLETS)). NLets is a not-for-profit law enforcement communications channel owned and governed by the States and available throughout the United States. This infrastructure includes the respective regional, State, and local networks of the participating agencies.

[9] Applicable opportunities and procedures are discussed in subsections 7.1 and 7.2 above.

[10] The ANSI/NIST standards define the content, format and units of measurements for the exchange of information that may be used in the fingerprint identification of a subject. These standards are intended for use in the interchange between criminal justice administrations or organizations that use an Automated Fingerprint Identification System (AFIS) and to provide a common interface for other AFIS and related systems worldwide.