Federal Bureau of Investigation

Privacy Impact Assessment
for the
Next Generation Identification System
Mobile Biometric Application Service

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

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

Date approved: [Component to insert date of PIA approval]

Section 1: Executive Summary

This Privacy Impact Assessment (PIA) is an update to the FBI's Criminal Justice Information Services (CJIS) Division's Mobile Biometric Application (MBA) PIA published in February 2019. The MBA Service consists of an application (i.e., "the MBA") on FBI-issued mobile devices (i.e., Bureau cell phones and tablets) and an MBA Web Server within the Next Generation Identification (NGI) System[1] that allows FBI agents and other authorized personnel to collect biometrics and associated biographic data. Previously, the FBI used the MBA Service only to collect fingerprints; now users have the ability to collect additional biometrics. The biometrics potentially collected consist of fingerprints, palm prints, iris images, face photos, and photos of scars, marks, and tattoos (SMT). A peripheral scanner must be plugged into the Bureau cell phone or tablet to collect the fingerprints, palm prints, and iris images. Photos of faces and SMTs are taken by the cameras integrated into the cell phones or tablets. For certain transactions, the MBA Service permits access, through NGI, to the Department of Defense's (DoD) Automated Biometric Identification System (ABIS), and the Department of Homeland Security's (DHS) Automated Biometric Identification System (IDENT).

Section 2: Purpose and Use of the Information Technology

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

The MBA Service is deployed within the FBI by authorized users including special agents, task force officers, Laboratory (Lab) Division staff, evidence response personnel, and security specialists. The MBA Service is used in situations and locations where mobile biometric identification is necessary or convenient (e.g., mass arrests, mass casualty incidents, natural disasters, rural areas, combat zones). The MBA Service may be used within the United States during investigatory detentions, incident to arrest, and when the subjects provide consent. The MBA Service is deployed outside of the United States to combat theatres such as Iraq and Afghanistan, and other hostile environments. FBI Legal Attaché offices are equipped with the MBA Service as well. Although the MBA Service is used largely for criminal justice and national security purposes, in some instances, it may assist with background checks of FBI employees and contractors, and to provide site security at FBI facilities or special event locations.

The MBA Service users collect biometrics and associated biographic information using an approved application operating on FBI-issued Android cell phones or tablets. Peripheral scanners are attached as needed to the cell phone or tablet. The Android devices are used by FBI personnel for a variety of official purposes; the MBA is one of many approved applications on the devices. The mobile devices connect to the CJIS Division via a secure Web Server, which is a protocol for transmitting messages securely over the Internet from the application to the NGI System.

The MBA Service only uses fingerprint capture devices on the Certified Products List [2] (i.e., products

[1] The NGI System is the FBI's national criminal history and biometrics repository. The various services, subsystems, and applications within the NGI System are covered by separate privacy documentation.
[2] *See:* https://fbibiospecs.fbi.gov

that comply with NGI specifications), and the application builds transactions that are compliant with the Electronic Biometric Transmission Specification,[3] the approved method for electronically communicating identity information to the NGI System. The transactions are sent via the secure Web Services to the NGI System from the application on the Android device for processing. Once submitted, the original transaction data collected by the MBA is no longer accessible via the mobile device. Once processing is complete, the NGI System stores any responses from NGI, IDENT, and ABIS until the MBA reaches out to retrieve them, which happens on an automated basis every 30 seconds. The NGI System sends the response back to the mobile device over the secure Web Services.

If there is a match in the NGI System, biometric, biographic, and event data will be returned to the MBA on the Bureau-issued cell phone or tablet. Event data consists of the criminal history record (i.e., "rap sheet") or civil information (i.e., background checks for purposes such as employment and licensing) maintained in the NGI System. If there is a match in IDENT or ABIS, only biographic and event data are returned. The system responses returned to the MBA will be retained within the application until deleted. The application is defaulted to automatically delete transactions after 30 days, but the MBA user may choose to delete sooner. The information is retained on the mobile devices for 30 days to permit the agent or other authorized user to return to the transaction if needed. The devices are frequently used in changing circumstances, such as overseas operations, where the user may need to retrieve a recent transaction. The MBA Service user may review the information within the application, but the mobile device does not automatically export the information to any other system.

All MBA Service collections must include tenprint fingerprints. These fingerprints are queried in the NGI System, ABIS, and IDENT consistent with the interoperability rules governing access to each system.[4] The NGI System maintains tenprint fingerprints associated with criminal, civil, and national security identities, and latent prints in the Unsolved Latent File (ULF).[5] ABIS includes fingerprints related to DoD's operations, such as military detainees and enemy combatants. IDENT includes fingerprints related to DHS's missions, such as homeland security, law enforcement, and immigration. When the NGI System is queried, the MBA Service user will be notified if there is a fingerprint match to the identity and will receive the subject's criminal history record, if one exists. A search of the NGI criminal repository is conducted with all MBA Service transactions and a search of the NGI civil repository is conducted with criminal arrest, unknown deceased, and access to FBI space transactions.

If the MBA Service user submits criminal fingerprints for retention (i.e., pursuant to arrest), the fingerprints and associated biographic information are retained in the NGI System. The fingerprints are searched in ABIS and IDENT but are only retained in those systems if they already contain independent encounter information regarding the subject. In addition, submission of criminal fingerprints, called the criminal booking transaction, requires the collection of a single frontal face photo. The submitted face photos are retained in the NGI System to augment the criminal arrest record. Currently, there is no face recognition capability within the MBA or the mobile device. The MBA Service user may subsequently request face recognition searches of collected photos through a

---

[3] *See:* https://fbibiospecs.fbi.gov/ebts-1/approved-ebts
[4] *See*: https://www.fbi.gov/file-repository/pia-next-generation-identification-biometric-interoperability.pdf/view
[5] *See:* https://www.fbi.gov/file-repository/pia-next-generation-identification-latent-services.pdf/view

separate process within the CJIS Division. [6] All criminal arrest photos collected with the MBA Service are enrolled in the NGI System's Interstate Photo System (IPS). The NGI IPS is the FBI's central repository of criminal photos that may be searched by law enforcement partners. [7]

For the criminal retain transactions, it is optional for the MBA Service user to collect palm prints, additional face photos, SMT photos, or iris images. If iris images are submitted, they are retained in the appropriate NGI System repository.[8] These additional biometrics are collected to augment the record and do not initiate separate biometric searches. The MBA Service user must also submit the following biographic information for criminal retain transactions: name, sex, hair color, eye color, weight, height, date of birth, race, and place of birth. The mobile device has the capability to scan the barcode on either a driver's license or passport. This feature automatically populates some of the required biographic information and eliminates manual entry and the potential for error. The agent must also include the "reason fingerprinted," with a transaction which is typically the arrest charge and/or the statute violated. This is required for all fingerprint submissions to the NGI System regardless of method of collection.

A deoxyribonucleic acid (DNA) sample is required to be collected pursuant to all federal arrests.[9] The mobile device may be used to scan the barcode from the DNA sample with the use of its camera. The barcode is translated into alphanumeric digits and stored in a miscellaneous field within the MBA submission. That alphanumeric code is retained within the NGI System and associates the DNA sample with the biographic data from the individual. It is important to note that this code is not the DNA profile of the individual and is used only by the Lab Division for expedited digital ingestion of the biographic data.

If a "query-only" criminal transaction is submitted, the MBA Service user is required to collect fingerprints and a front profile picture. No other biometrics are mandatory for this transaction and no biographic data is required. The fingerprints are searched against existing holdings, including the ULF, but are not retained in the NGI System, ABIS, or IDENT operational environments. If a deceased unknown transaction is submitted, the MBA Service user is required to collect fingerprints, a photo, and limited biographic information, such as sex, hair and eye color, height, and weight. The fingerprints and associated information are retained in the NGI System and flagged as deceased unknown.. These submissions are searched in ABIS and IDENT but are only retained if those systems already contain independent encounter information regarding the subject.

When an MBA Service user submits a civil transaction, such as a background check, only fingerprints are required. These civil transactions are searched and retained within the NGI System but are not searched against any other system. The MBA Service user must submit biographic and event data consisting of name, sex, hair color, eye color, weight, height, date of birth, race, place of birth, reason fingerprinted, and case number.

Some MBA Service collections are sent to the Lab Division rather than the CJIS Division. If an FBI

---

[6] *See*: https://www.fbi.gov/file-repository/pia-face-operations-services.pdf/view
[7] *See*: https://www.fbi.gov/file-repository/pia-ngi-interstate-photo-system.pdf/view
[8] *See*: https://www.fbi.gov/file-repository/pia-ngi-iris-service.pdf/view
[9] *See*: https://www.fbi.gov/file-repository/pia-combined-national-deoxyribonucleic-acid-dna-index-system-codis-031423.pdf/view

elimination transaction is submitted, the MBA Service user is required to collect only fingerprints but may choose to submit a photo. Elimination fingerprints are taken to eliminate innocent people from an investigation (e.g., fingerprints taken from bank employees after a bank robbery). These transactions are not submitted to the NGI System or any other system, but are sent directly to the Lab Division for comparisons of latent prints from crime scenes. For latent print collection, the MBA Service user takes a photo of the latent print. The mobiledevice includes technical controls that will not allow collection of the photo unless the picture is in focus and of the appropriate aspect ratios. The MBA Service user is required to include a latent identification number, assigned by the evidence response team, and a description of where the latent print was collected when submitting the photo to the Lab Division. The latent print transactions are not searched in any system and are generally used by FBI evidence response personnel. Transactions are submitted from the mobile device to the secure Web Server within the NGI System and then routed to a mail bucket for Lab examiners to retrieve the transaction for review.

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

Authority	Citation/Reference
Statute	8 U.S.C. §§ 533, 534
Executive Order	
Federal regulation	28 CFR § 0.85
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

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

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	*X*	A,B,C,D	
Date of birth or age	*X*	A,B,C,D	
Place of birth	*X*	A,B,C,D	
Sex	*X*	A,B,C,D	
Race, ethnicity or citizenship	*X*	A,B,C,D	
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	*X*	A,B,C,D	The SSN is required for MBA civil submissions but may also be collected for criminal transactions. Criminal history returned to the MBA user from the NGI System typically contains the SSN.
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
E-mail addresses (personal, work, etc.) Please describe in Comments			
Phone numbers (personal, work, etc.) Please describe in Comments			
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A,B,C,D	
Juvenile criminal records information	X	A,B,C,D	as permitted by federal and state law
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	A,B,C,D	
- **Video containing biometric data**			
- **Fingerprints**	X	A,B,C,D	
- **Palm prints**	X	A,B,C,D	
- **Iris image**	X	A,B,C,D	
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**	X	A,B,C,D	
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Other: height, weight, hair & eye color; DNA, barcode for passport & driver's license**	X	A,B.C.D	
System admin/audit data:			
- **User ID**	*X*	A	
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**	*X*	A	
- **Queries run**	X	A	
- **Content of files accessed/reviewed**	*X*	A	
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			

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

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

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

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

Other (specify):

Section 4: Information Sharing

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

Generally, the information collected from the individual will route directly to the NGI System and not be shared separately via the mobile device; however, if the FBI agent or other authorized user determines that the information is relevant to a law enforcement or national security investigation, the information may be subsequently shared pursuant to investigative authorities.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X			
DOJ Components	X			
Federal entities	X			
State, local, tribal gov't entities	X			
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments	X			
Foreign entities				
Other (specify):				

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

The biometrics maintained within the NGI System, including those submitted via the MBA Service for retention, may be used for FBI research and development purposes in accordance with applicable

federal law and regulations. The FBI has a longstanding relationship with the National Institute of Standards and Technology (NIST) to perform biometric testing. When the FBI provides data to NIST, it is subject to strict security and use protections pursuant to an interagency agreement between the two agencies. Additional protections are delineated in "Government Furnished Information" letters which the FBI provides to NIST regarding specific research projects and data sets. Any fingerprints used for research and development would be sent without other associated PII; however, some non-unique biographic information such as year of birth and sex, as well as other biometrics may accompany the fingerprints if required by the specific research activity. The data is encrypted in accordance with Federal Information Processing Standards 140-2 requirements prior to release. The data is stored in FBI laboratories which have received an authority to operate in accordance with FBI security policy and the Federal Information Security Modernization Act. In addition, only those with documented authorization and a true need-to-know are granted access to the data. No biometrics collected via the MBA Service are released to the public for "open data" purposes.

Section 5: Notice, Consent, Access, and Amendment

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

No Privacy Act notice is provided to individuals regarding the collection, use, and sharing of their criminal or national security fingerprints and associated biometric and biographic information in the NGI System. The applicable FBI systems of records have been exempted from the requirement of 552a(e)(3) for the criminal and national security records maintained in the NGI System pursuant to the provisions of 552a(j) and (k) of the Act. Except for instances of latent print collection, the individual will be present when their biometrics are captured, and will be informed by the MBA Service user as to the purpose of the collection. A written Privacy Act notice is provided by the MBA Service user to individuals when fingerprints are collected for retention in the NGI System for civil purposes, such as employment. The NGI System's SORN provides general notice in the Federal Register of the collection and use of fingerprints and associated information. The most current version may be found at 84 Fed. Reg. 54,182 (October 9, 2019). This PIA also provides general information to the public, as does the previously published PIAs regarding the NGI System, which may be found at https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments.

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

An individual submitting civil fingerprints, such as for employment, voluntarily provides their fingerprints to obtain the relevant benefit, and receives a notice pursuant to 552a(e)(3) of the Privacy Act.

Privacy Act Subsection (e)(3) notices are generally not required solicitations of information from individuals as part of criminal or national security investigations. An individual whose

fingerprints and associated biometrics/biographics are collected via the MBA Service during investigatory detention or incident to arrest in connection with a criminal or national security investigation has no opportunity to refuse the collection of his or her personal information. When fingerprints and associated biometrics/biographics are collected as part of a criminal or national security investigation, but not connected with investigatory detention or incident to arrest, agents will only procure biometrics through the MBA Service with the consent of the individual.

Regarding use and further dissemination of collected information, federal agency criminal or national security uses of the information in the NGI System must comply with the provisions of applicable law, including the Privacy Act.

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

As noted above, the FBI maintains exemptions from access and amendment provisions of the Privacy Act for certain records maintained in the NGI System. However, title 28 CFR part 16, subpart A, provides general guidance on access to information in FBI files pursuant to the Freedom of Information Act; and 28 CFR part 16, subpart D, provides general guidance regarding access to, and amendment of, information in FBI files to the extent it is available pursuant to the Privacy Act. In addition, title 28 CFR 16.30-16.34 establishes specific procedures for an individual to obtain a copy of his or her criminal history record from the NGI System for review and correction.

Section 6: Maintenance of Privacy and Security Controls

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

	The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):
X	The NGI ATO was granted on January 9, 2023 and is valid until January 8, 2026. The MBA Web Server is within the NGI ATO. A security risk assessment was conducted for the NGI ATO, which included the Web Server used by the MBA. The FBI-issued mobile devices are under the Mobile Unclassified Development Enterprise (MUDE) ATO. The MUDE system covers all Bureau mobile devices and provides mobile device and application management services and application deployment. The MUDE ATO was granted on April 12, 2024 and is valid until November 11, 2025. The MBA was also specifically approved pursuant to an FBI security policy for the use of mobile applications.

	If an ATO has not been completed, but is underway, provide status or expected completion date: **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** No POAMs related to privacy controls.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** For the NGI System, confidentiality, integrity, and availability is high across all categories. Law enforcement agencies require access to this information in a timely and accurate manner and confidentially must be maintained to those members of the user community with a need to know this information. For the MUDE system, confidentiality, integrity, and availability is moderate across all categories. The MBA Service has been assigned high security categories, similar to the NGI System.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The NGI System, including the MBA Web Server, and the MUDE System (i.e., the Bureau mobile devices) are continually monitored at the host and network layer. FISMA policy compliance testing occurs monthly.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** Host operating system logs are consolidated into the CJIS enterprise system audit consolidation and monitored for irregular activities or compliance failures. The NGI System Security Administrator reviews security-related logs on a weekly basis. Similar controls are in place for the MUDE at the host level.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** Pursuant to the CJIS Security Policy, law enforcement users receive security/privacy training as an initial requirement of access to the NGI System, and annually thereafter. Users of the MBA Service receive specific instruction on the permissible use of the application and the FBI-issued mobile devices. All MBA users have undergone privacy, security, and investigatory training

	to ensure that information submitted to and retrieved from the NGI System is properly handled.

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

The MBA Service implements privacy-specific safeguards as controls for protecting the confidentiality of personally identifiable information (PII). The mobile devices comply with all FBI security policies and protocols regarding system security, including security countermeasures that hold all users accountable for their actions while on the computer system and ensuring access control techniques are utilized. Security controls for the MBA Service are implemented to protect data that is processed, stored, or transmitted by the application. The FBI mandates the use and compliance with security controls listed in NIST SP 800-53 to address general protections of data and systems. The items listed below are some of the NIST SP 800-53 controls that are assessed to help safeguard the confidentiality of PII on mobile devices:

- Access Enforcement (AC-3) - Account creation and logical access are managed according to the account management policy. Functional managers request/approve accounts according to this policy.
- Least Privilege (AC-6) — Role-based Access Control (RBAC) is strictly defined, enforced and documented according to policy.
- Audit Review, Analysis, and Reporting (AU-6) - Automated mechanisms are in place to detect and identify and report suspicious activity which would then trigger supplemental manual processes for review and analysis. Automated daily reports for the application show failed login attempts and all transmissions for manual review of misuse.

The MBA Service is only available to FBI agents and authorized personnel who have been issued FBI mobile devices. Processes are in place to ensure that only authorized users have access to the mobile devices. Access to these mobile devices is via passcode or fingerprint. MBA users must comply with the FBI's *Mobile Devices and Mobile Applications Policy Guide*, which contains the FBI's requirements for the management of FBI-owned mobile devices. User activity is audited by system administrators on a routine and event-driven basis. Only system administrators may establish user accounts. Information security requirements and standards for the Android cell phones and tablets are established and maintained by the OCIO of the FBI. The MBA is logically separated from other storage capabilities of the mobile device, and prevents the local storage of information in the device's camera roll or other applications. The mobile devices are approved to process sensitive unclassified information, such as PII

Access to the MBA Service is managed by the CJIS Division, who sets up the user's account and manages the program. The MBA accounts are configured, managed, and accepted by the MBA Web Server within the NGI ATO boundary. Web service logs and transaction logs are maintained

in accordance with NGI System rules. The MBA requires a username and password in addition to the access requirements of the mobile device. The MBA has a dedicated URL to transmit data to the MBA Web Server pre-configured in its settings, along with a default password for initial configuration/authentication purposes. The MBA sends the user's fbi.gov email address and a unique configuration ID from the mobile device to the MBA Web Server for authentication. A token and date/time stamp is created and used for authentication. The MBA re-authenticates the user every time the mobile device connects to the Web Server and a warning banner is visible every time the user authenticates. The user must enter the configuration ID every time he/she accesses the MBA and, at that time, the warning banner appears.

The MBA Web Server also manages the biometric submissions and responses from/to the MBA on the mobile devices. The MBA controls the biometric collection, including any data from the external devices (e.g. scanner) attached to the mobile device. The MBA sends the EBTS compliant biometrics to the MBA Web Server and the user will receive a notice on the MBA if the biometrics were successfully submitted. The response from the NGI System to the MBA is routed through the MBA Web Server. The user must have the configuration ID to view the response in the MBA. The length of time the response remains on the mobile device depends on the configuration settings or user discretion. The configuration ID is embedded in the EBTS transaction in the submission field to allow detailed reporting and track individual transactions without storing any user information in the NGI System. Although the MBA enhances the efficiency and effectiveness of biometric collection and has a secure exchange with the MBA Web Server, the data on the mobile device is dependent largely on the security of the device.

The MBA was tested by the FBI's Information Technology Engineering Division and approved to be "white-listed". Once an application is white-listed, it is placed within the FBI application catalog for use on FBI-issued mobile devices. However, FBI personnel cannot open and utilize the MBA unless an individual account has been requested and approved by the MBA team. The CJIS Division has requested a new review of the MBA through the Mobile Application Review and Approval Process that is replacing the earlier "white-list" process. In the interim, the Information System Security Manager (ISSM) and Office of the Chief Information Officer (OCIO) staff have reviewed the security of the MBA and its Web Server within the NGI System. The ISSM found that the data is properly encrypted at rest and in transmission and that the risk to the data and to the NGI System is low.

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

All biometric and associated information collected by the FBI agent or authorized user, and all information returned to the user from the NGI System, ABIS, and IDENT, will be deleted from the mobile devices within 30 days. The data retention on the mobile device is a configurable setting established by the system administrator, set for an auto-delete of 30 days. If the agent submits a "query-only" transaction, the fingerprints are not retained in the NGI System, ABIS or IDENT; however, if the agent submits criminal fingerprints for retention, the fingerprints and associated

information are retained in the NGI System similar to any traditional criminal booking transaction within the NGI System. The fingerprints are only retained in IDENT or ABIS if those systems have independent encounter information regarding the individual. If any information is retained in the NGI System, the National Archives and Records Administration approved the destruction of fingerprint cards and associated information, including other biometrics, when criminal and civil subjects attain 110 years of age, or seven years after notification of death with biometric confirmation. Likewise, if any information is retained in ABIS or IDENT, the information would be retained according to the records retention schedules of DoD and DHS.

Section 7: Privacy Act

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

_____ No. __X__ Yes.

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

The NGI System: 81 Fed. Reg. 27,284 (May 5, 2016); 82 Fed. Reg. 24151, 156 (May 25, 2017); 84 Fed. Reg. 54,182 (Oct. 9, 2019)

The FBI Central Records System, 63 Fed. Reg. 8659, 671 (Feb. 20, 1998), as amended at 66 Fed. Ref. 8425 (Jan. 31, 2001), 66 Fed. Reg. 17200 (Mar. 29, 2001), and 82 Fed. Reg. 24147 (May 25, 2017)

Section 8: Privacy Risks and Mitigation

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

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

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

The information collected by the mobile devices, unless retained in the NGI System, is generally available only to FBI agents and other authorized FBI users who require the information in the

furtherance of their investigations or other official duties. Fingerprints and associated biometric and biographic information are collected by the MBA, an application that sits on Bureau-issed mobile devices. The application is subject to FBI security reviews and policy; the mobile devices are covered by an appropriate ATO and subject to security and use policy. The MBA Service user determines the necessary information to collect based on his/her law enforcement training, the MBA Service user rules, and the nature of the encounter with the individual. The biometric and/or biographic information is provided by the individual; therefore, he/she has knowledge of all personal information being collected. The tenprint fingerprints are used to establish positive identification, which greatly eliminates the risk of misidentification. The fingerprints search the NGI System and other federal biometric systems for any criminal history or other derogatory information. The data obtained from the NGI System requires the submission of biometrics and only that subject's data is returned to the MBA Service user.

When the MBA transaction is submitted to the NGI System, the information is sent in encrypted format via the secure Web Server. The data retention on the mobile device is a configurable setting established by the system administrator, set for an auto-delete of 30 days. The information remains on the mobile devices for a very limited time period, which mitigates the possibility of unauthorized disclosure. If the agent submits a "query-only" transaction, the fingerprints are not retained in the NGI System, ABIS or IDENT; however, if the agent submits criminal fingerprints for retention, the fingerprints and associated information are retained in the NGI System. The fingerprints are only retained in IDENT or ABIS if those systems have independent encounter information regarding the individual. Any information that is retained in the NGI System, ABIS, or IDENT is maintained according to those systems' security and use policies, which are quite robust as they are the U.S. government's largest and most trusted biometric systems.

The collection and searching of the biometric and biographic information present privacy risks that the personal information of individuals will be searched or disseminated for improper purposes, or that there will be improper access to or misuse of the information. This risk is significantly mitigated because MBA Service users must comply with numerous investigative and security policies and guidance issued by the FBI, as well as the Privacy Act of 1974, and all relevant laws and policies. In other words, the FBI agent or other authorized user who is collecting the information has received significant investigatory and legal training and is subject to extensive oversight. In addition, they must comply with specific legal guidance regarding the domestic use of the MBA and must follow guidance issued by the MBA program for the appropriate use of the application and the mobile devices.

When an MBA account is created, the user is provided a copy of the internal legal guidance on the permitted use of the MBA, and a detailed step-by-step guide on how to correctly submit MBA transactions. The MBA program conducts transaction reviews to ensure that the appropriate reason fingerprinted is associated with the MBA submissions. As needed, the MBA program will reach out directly to users to provide any needed information or clarity to ensure the accuracy of transactions. The MBA program monitors the submission of fingerprints real-time. If the fingerprints are poor quality, the program will reach out to the user to assist with capturing fingerprints that will be accepted by the NGI System. The MBA program also travels on a regular basis to FBI Field Offices to provide training on how to collect quality fingerprints and other biometrics.

Further, automated security mechanisms are in place to detect and identify suspicious activity which would trigger supplemental manual review. Automated daily reports show failed log in attempts and all transmissions for review of misuse. The MBA Service users are notified that they are accessing a U.S. government information system and that it is provided for U.S. government-authorized use only and unauthorized or improper use may result in disciplinary action and civil and/or criminal penalties. By using this information system, MBA Service users understand and consent that they have no reasonable expectation of privacy regarding any communications transmitted through or data stored on the information system and that any time, the government may monitor, intercept, or search and/or seize data transiting or stored on the information system. Specific to the MBA, a disciplinary policy is included within the notification banner.

Finally, FBI management has implemented safeguards for PII protection such as standard operating procedure and policy requirements, education, training, and awareness. These safeguards are combined with relevant and related IT security controls as part of a comprehensive privacy program. Users are subject to Annual Security Awareness training that includes how to identify and protect PII. The required annual training refresher also serves to reinforce policies and procedures, such as access rules, retention schedules and incident response. The MBA program implements privacy-specific safeguards as controls for protecting the confidentiality of PII, such as strict user account management, the IT security protections of the MBA device, and encryption of MBA data.