Federal Bureau of Investigation

Privacy Impact Assessment
for the
Mobile Biometric Application

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

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

Date approved: February 12, 2019

(May 2015 DOJ PIA Form/FBI revision August 1, 2017)

EXECUTIVE SUMMARY

This Privacy Impact Assessment (PIA) describes the FBI's Criminal Justice Information Services (CJIS) Division's Mobile Biometric Application (MBA) program. The MBA program consists of applications on mobile devices (i.e. cell phones and tablets) that allow FBI agents and other authorized personnel to collect fingerprints, photos, and available biographic data to confirm an individual's identity. A fingerprint scanner must be plugged into the cell phone or tablet in order to collect the fingerprints. The MBA program enables instant access to the following federal biometric databases: the FBI's Next Generation Identification (NGI), the Department of Defense's Automated Biometric Identification System (ABIS), and the Department of Homeland Security's Automated Biometric Identification System (IDENT).

Section 1: Description of the Information System

(a) the purpose that the records and/or system are designed to serve:

MBA devices are used by FBI agents and federal task force officers (TFOs) in situations and locations where mobile biometric identification is necessary (e.g. mass arrests, natural disasters, combat zones). The MBA devices may be used within the United States during investigatory detentions, incident to arrests, and when the subjects provide consent. The MBA devices are also deployed outside of the United States to combat theatres such as Iraq and Afghanistan, and other hostile environments. Although the MBA devices are used largely for criminal justice and national security purposes, in some instances, they may be used to assist with background checks of FBI employees and contractors, and to provide site security at FBI facilities and/or special event locations.

(b) the way the system operates to achieve the purpose(s):

The FBI agents and TFOs collect tenprint fingerprints using a fingerprint scanner and an approved application operating on FBI-issued Android smartphones or tablet devices. The Android devices are used by FBI personnel for a variety of official purposes; the MBA program is only one approved operational use. The MBA devices connect to CJIS via a secure Web Services, which is a protocol for transmitting messages securely over the Internet from the application to the NGI system. The fingerprints are queried in NGI, ABIS and IDENT, consistent with the interoperability rules governing access to the systems. When NGI is queried, the agent 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 transaction types and a search of the NGI civil repository is conducted with select transactions, such as criminal arrests, unknown deceased,

and access to FBI space. If there is a match in ABIS and/or IDENT, biographic and event data[1] contained in the respective system will be returned to the agent.

Photos, including face and iris images, may be collected but are not required. All photos must be associated with fingerprints. The photos are collected for retention in NGI to augment the arrest record; however, face or iris recognition technology cannot be generated from the mobile application. Should the mobile application be used in conjunction with such facial recognition technology, updated privacy documentation would be necessary.

(c) what type of information is in the system:

The information collected and entered into the MBA devices will be retained within the application until it is deleted. The application is defaulted to automatically delete transactions after 30 days but the agent may choose to delete sooner. The information is retained on the MBA devices for 30 days in order to permit the agent to return to the transaction if needed. The devices are frequently used in circumstances that fluctuate, such as overseas operations, and an agent may need to retrieve a recent transaction. If the agent submits a "query-only" transaction, the fingerprints are not retained in NGI, ABIS and IDENT; however, if the agent submits criminal fingerprints for retention (i.e. pursuant to arrest), the fingerprints and associated information are retained in NGI. The fingerprints are only retained in IDENT or ABIS if those systems have independent encounter information regarding the subject (such as if, previously, DOD or DHS had separately encountered that same individual and already had that individual's information in IDENT or ABIS).

(d) who has access to information in the system:

At this time, the MBA program is only available to FBI agents and TFOs.

(e) how information in the system is retrieved by the user:

If there is a match in NGI, ABIS and/or IDENT, biographic and event data contained in the respective system will be returned to the agent's MBA device. The agent may review the information within the application but the device does not automatically export the information.

(f) how information is transmitted to and from the system;

The MBA uses fingerprint capture devices on the Certified Products List (products that comply with NGI specifications), and the application builds transactions that are compliant with the Electronic Biometric Transmission Specification, the method for electronically communicating identity information to NGI. The transactions are sent via the secure Web

[1] Examples of event data include contextual information such as a border stop for IDENT, or an overseas encounter for DoD.

Services to NGI from the application on the Android device for processing. Once processing is complete, NGI stores any responses from NGI, IDENT, and ABIS until the application reaches out to retrieve them, which happens on an automated basis every 30 seconds. NGI sends the response back to the Android device over the secure Web Services.

(g) whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects); and

The MBA devices connect to NGI via Web Services. NGI is the FBI's biometric system that maintains criminal history records with associated tenprint criminal fingerprints. It also retains civil and latent fingerprint repositories, and associated biometrics, such as photos and palmprints.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security	X	Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID		Credit card			
Other identifying numbers (specify):					

General personal data					
Name	X	Date of birth	X	Religion	
Maiden name	X	Place of birth	X	Financial info	
Alias	X	Home address		Medical information	
Gender	X	Telephone number		Military service	
Age		Email address		Physical characteristics	
Race/ethnicity	X	Education		Mother's maiden name	
Other general personal data (specify):					

Work-related data					
Occupation	X	Telephone number		Salary	
Job title		Email address		Work history	
Work address		Business associates			
Other work-related data (specify): Occupation information may be collected when the MBA devices are used for civil purposes.					

Distinguishing features/Biometrics					
Fingerprints	X	Photos	X	DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	X
Voice recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify):					

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	X
IP address		Queries run		Contents of files	
Other system/audit data (specify): Web Service logs and transaction logs are maintained in accordance with NGI system rules and logs are not disseminated.					

Other information (specify)

2.2 Indicate sources of the information in the system. (Check all that apply.)

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

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

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

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats

to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Fingerprints, photos, and associated biographic information are collected and entered into the MBA device. The agent determines the necessary information to collect based on his/her law enforcement training 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 and to search NGI and the other biometric systems for any criminal history or other derogatory information. When the MBA transaction is submitted to NGI, the information is sent in encrypted format via the secure Web Services. The data retention on the application 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 NGI, ABIS or IDENT; however, if the agent submits criminal fingerprints for retention (e.g. pursuant to arrest), the fingerprints and associated information are retained in NGI. The fingerprints are only retained in IDENT or ABIS if those systems have independent encounter information regarding the individual.

The collection and searching of the biometric and biographic information presents 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 agents and TFOs must comply with numerous investigative 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 TFO 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 devices and must follow guidance issued by the MBA program for the appropriate use of the devices. 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.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose

X	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities		For administrative matters
X	To conduct analysis concerning subjects of investigative or other interest	X	To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
X	Other (specify): security vetting and FBI employment		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

As listed below, the FBI has statutory authority to collect, preserve, and exchange biographic and biometric information for criminal and national security purposes. In compliance with this authority, FBI agents and TFOs use MBA devices to confirm the identity and assess the threat of individuals in settings which require the use of mobile devices. The agents do not collect any information via the MBA devices that would not be permitted via a non-mobile device, such as a computer or fingerprint scanner at a stationary work location. By using the MBA devices, the agents receive accurate and timely information that adds value to the FBI's mission to fight crime and terrorism and that assists with agent safety.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

Authority		Citation/Reference
X	Statute	28 U.S.C. §§533, 534
	Executive Order	
X	Federal Regulation	28 CFR 0.85
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

3.4 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National

Archives and Records Administration, if available.)

All biometric and associated information collected by the agent or TFO, and all information returned to the agent from NGI, ABIS, and IDENT, will be deleted from the MBA devices within 30 days. If any information is retained in NGI, 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.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.) [In addition to providing a narrative answer, please consult the ISSO/ISSM for the system's NIST 800-122 PII Confidentiality Risk Level, and check the applicable Confidentiality Safeguard Security Controls.]

The MBA program is limited to authorized users who possess accounts within the MBA application. The MBA program is subject to extensive security protections, access limitations, and quality control standards. Processes are in place to ensure that only authorized users have access to the MBA devices. All MBA users have undergone privacy, security, and investigatory training to ensure that information is properly handled. MBA users must comply with the 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 smartphone must be established and maintained by the Mobility Program Office (MPO) and Security Division of the FBI.

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.

PII Confidentiality Risk Level:

☐ **Low** ☑ **Moderate** ☐ **High**

- Is the system protected as classified; or
- Does the system involve intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system; or
- Is the system critical to the direct fulfillment of military or intelligence missions (excluding routine business or administrative applications, e.g., finance, logistics, personnel management)?

☐ **Yes** ☑ **No**

If Yes, the system meets the NIST 800-59 definition of a National Security System.

Access controls

X	Access Enforcement: the system employs role-based access controls and enforcement mechanisms for PII. The Android smartphones and tablets are managed and controlled by the Mobile Device Manager (MDM) within the MPO. Other than system administrators, all users of the MBA devices are general users.
X	Separation of Duties: users of de-identified PII data are not also in roles that permit them to access the information needed to re-identify the records. Other than system administrators, MBA users are all general users.
X	Least Privilege: user roles enforce the most restrictive set of rights/roles for each user group. Other than system administrators, MBA users are all general users.
X	Remote Access: remote access is prohibited or limited to encrypted communication channels. There is no remote access to the MBA devices.
X	User-Based Collaboration and Information Sharing: automated mechanisms are in place for matching PII access authorizations to access restrictions, such as contractual/MOU/MOA requirements. The MBA program does not support this type of information sharing.
X	Access Control for Mobile Devices: Yes, the Android smartphones and tablets are properly secured with access limited to FBI agents and TFOs.

Audit controls

X	Auditable Events: access to PII is audited for unauthorized access.
X	Audit Review, Analysis, and Reporting: audit records are regularly reviewed for inappropriate or unusual activity affecting PII; such activity is investigated and reported; and responsive action and appropriate mitigation is taken. For the Samsung smartphone and tablet, logging occurs on the MDM Server and they are accessible by request.

Identification and Authentication controls

	Identification and Authentication: Users are uniquely identified and authenticated before accessing PII; remote access requires 2-factor authentication.
[Explain how the privacy risks associated with controls not checked are otherwise mitigated.] Once an individual installs the application on his/her MBA device, a unique user account will be created.	

The user's access is authenticated by the assigned unique configuration ID, as well as the user's Bureau email which is assigned to the device.

Media controls

N/A	Media Access: access to system media (CDs, USB flash drives, backup tapes) is restricted.
N/A	Media Marking: media containing PII is labeled.
N/A	Media Storage: media containing PII is securely stored.
N/A	Media Transport: media is encrypted and stored in a locked container during transport.
N/A	Media Sanitation: media is sanitized prior to re-use.
[Explain how the privacy risks associated with controls not checked are otherwise mitigated.] There is no media access to the Android phones or tablets.	

Data Confidentiality controls

X	Transmission Confidentiality: information is encrypted prior to transmission or encrypted transmission is used. (**Required if the system meets the NIST 800-59 definition of a National Security System**.) Yes, it is encrypted on all MBA devices.
X	Protection of Information at Rest: information stored on a secondary storage device (e.g., hard drive or backup tape) is encrypted. (**Required if the system meets the NIST 800-59 definition of a National Security System**.) Encryption is managed by the MBA device and the data on the application is encrypted while it resides on the phone or tablet. When the data is transmitted to and from CJIS, it travels over a secure web service.

Information System Monitoring

X	Information System Monitoring: network boundaries are automatically monitored for unusual or suspicious transfers or events. Yes, this is managed and monitored by the MDM and the Enterprise Security Operations Center (ESOC) for both the phones and tablets.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	X			
DOJ components	X			

Federal entities	X			
State, local, tribal gov't entities				
Public				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

Generally, the information collected from the individual will not be shared via the MBA program; however, if the FBI agent or TFO determines that the information is relevant to a law enforcement or national security investigation, the information may be shared pursuant to investigative authorities.

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.) [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

The information collected by the MBA devices is generally available only to authorized FBI agents and TFOs who require the information in the furtherance of their investigations. The information remains on the devices for a very limited period of time, which mitigates the possibility of unauthorized disclosure. Information may be provided via NGI to others within the FBI and DOJ components when there is a need for the information to perform official duties, pursuant to 28 U.S.C §534 and 5 U.S.C. §552a(b)(1). Any information that is retained in NGI, 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 biometric systems.

The MBA device 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 criminal penalties. By using this information system, 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 devices, a disciplinary policy is included within the notification banner.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7. Additional notice is provided with this PIA.	
X	Yes, notice is provided by other means.	Specify how: Applicants will be provided with notice via fingerprint cards, live-scan fingerprint devices, and/or other publications. Specific notice and consent is not provided to individuals whose prints are obtained pursuant to criminal and national security investigations.
	No, notice is not provided.	Specify why not:

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

X	Yes, individuals have the opportunity to decline to provide information.	Specify how: Please see 5.1
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: Please see 5.1

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

X	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how: Please see 5.1
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Please see 5.1

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why

not.

A person under arrest or the subject of a criminal or national security investigation generally has no opportunity or right to refuse the collection of biometrics. However, in circumstances where the information is collected directly from the individual, the open and obvious act of fingerprint collection itself in which the individual participates provides notice of the collection. In addition, the privacy risks associated with lack of notice to affected individuals about the collection, maintenance, or use of biometrics are mitigated by the general notice to the public via the FBI's published SORNs, PIAs, and other Privacy Act notices. The risk of erroneous information is mitigated because the FBI is collecting the information directly from the individual and the FBI has a substantial interest in ensuring the accuracy of information in the system, and in taking action to correct any erroneous information of which it may become aware. Additionally, the risk is mitigated because the maintenance and dissemination of information must comply with the provisions of any applicable law, regulation, or policy, including the Privacy Act. Title 28 C.F.R., part 16, subpart A, provides general guidance on access to information in FBI files pursuant to the Freedom of Information Act, and 28 C.F.R., part 16, subpart D, provides general guidance regarding access to, and amendment of, information in FBI files pursuant to the Privacy Act. In the limited instances that the MBA devices are used to perform site security checks or background checks for employment or access, a Privacy Act notice is provided at the time of fingerprinting.

Section 6: Information Security

6.1 Indicate all that apply.

x	A security risk assessment has been conducted. A security risk assessment was conducted for the NGI ATO, which included the Web Services used by the application, but not the application itself. The application and the mobile devices were approved pursuant to an FBI security policy for the use of mobile devices and applications. The date of that approval was February 2016.
x	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: These are covered with the NGI ATO and the security testing pursuant to the FBI requirements for the use of mobile devices and applications.
x	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: The MPO has vetted, tested, approved and whitelisted the MBA program application. The MPO ensures that the MBA devices are covered by the MDM for security. The Web Services has been tested pursuant to the NGI ATO.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: The NGI ATO was granted in October 2018 and is valid until 2020. The application and devices do not have their own ATOs, but undergo separate security testing.
x	Auditing procedures are in place to ensure compliance with security standards. System Administrators review access logs regarding the mobile devices, application, and Web Services to identify attempts by unauthorized users.

x			Contractors that have access to the system (i.e. the the mobile devices, application, and Web Services) are subject to provisions in their contract binding them under the Privacy Act.
x			Contractors that have access to the system (i.e. the the mobile devices, application, and Web Services) are subject to information security provisions in their contracts required by DOJ policy.
x			The following training is required for authorized users to access or receive information in the system (i.e. the the mobile devices, application, and Web Services):
	x		General information security training
	x		Training specific to the system for authorized users within the Department.
			Training specific to the system for authorized users outside of the component.
			Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure. [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

The MBA program implements privacy-specific safeguards as controls for protecting the confidentiality of PII. MBA devices are in compliance with all FBI security policies and protocols regarding system security, including (1) security countermeasures that hold all users accountable for their actions while on the computer system, (2) ensuring access control techniques are utilized, by the implementation of a management-approved Standard Operating Procedures guide for supervisors and staff, (3) utilizing security controls such as internal labeling of contents by classification labeling.

Security controls for the MBA are implemented to protect data that is processed, stored, or transmitted by the system. 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 MBA 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 Web Server also has security mechanisms in place to see any attempt to breach and will appear in the daily logs.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: FBI Central Records System, 63 Fed. Reg, 8659,671 (February 20, 1998) as amended; and Next Generation Identification System, 81 Fed. Reg. 27,284 (May 5, 2016); 82 Fed. Reg. 24151, 156 (May 25, 2017).
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

The information submitted by the FBI agent or TFO to the MBA device may include the individual's place of birth or citizenship status, as this information may assist with the searching of federal databases. However, information in the MBA device and in NGI pertaining to U.S. citizens and permanent resident aliens is generally not retrieved based on citizenship; rather, the information is retrieved based on biometrics and personal identifiers, as described above in Section 1, "Description of the Information System."