Federal Bureau of Investigation

Privacy Impact Assessment
for the
Facial Analysis, Comparison, and Evaluation (FACE)
Operations Services

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: 6/24/2024

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

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

This Privacy Impact Assessment (PIA) is an update to the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit PIA published in May 2015 and the FACE Phase II System PIA published in July 2018. The FACE Operations Services within the Investigative Services Support Unit in the FBI's Criminal Justice Information Services (CJIS) Division provides automated searching and manual review of investigative photographs collected by FBI personnel against authorized photograph repositories collected by the FBI and other government agencies. This PIA addresses the activities of FACE Operations Services and its case management system, named the FACE Case Management System (FCMS), which is an automated workflow management tool to document the details of all work transactions and to process and communicate face recognition (FR) requests.

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 FACE Operations Services provides investigative lead support to FBI Field Offices, Operational Divisions, and Legal Attachés by comparing the face images of persons associated with open FBI assessments[1] and investigations[2] against facial images available in federal and state FR systems. In limited instances, the FACE Operations Services provides FR support for closed FBI cases (e.g., missing and wanted persons). The FACE Operations Services requires an open assessment or investigation in accordance with the Attorney General Guidelines for Domestic FBI Operations (AGG-DOM) and the FBI Domestic Investigations and Operations Guide (DIOG). The FACE Operations Services provides unique and significant assistance to FBI personnel that cannot be accomplished by other investigative methods.

Currently, the FACE Operations Services offers its support and expertise only internally within the FBI. In the future, FR support may be offered to other law enforcement (LE) components within the Department of Justice (DOJ). If so, the FACE Operations Services will only offer support with photographs that have been obtained in compliance with applicable law and policy.

---

[1] Assessments may be opened to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security. They must have an authorized purpose and clearly defined objectives; they cannot be arbitrary or based on speculation.

[2] Preliminary investigations may be opened on the basis of "allegation or information" indicative of possible criminal activity or threats to the national security. Full investigations may be opened when there is "an articulable factual basis" of possible criminal or national threat activity.

In its support of assessments and investigations, the FACE Operations Services accepts unclassified photographs of subjects of, and persons relevant to, open FBI cases via the FCMS.[3] These photographs are called "probe photographs." Upon receipt of a probe photograph, the FACE Operations Services uses automated FR software developed and built by the FBI to compare the probe photograph against photographs contained within government photograph systems. The FACE Operations Services does not search probe photographs against any private, public, or non-governmental photograph system. Federal photograph repositories include the photographs collected by FBI, law enforcement, and other federal partners[4] maintained in the FBI's Next Generation Identification (NGI) Interstate Photo System (IPS)[5], the visa and passport photographs maintained by the Department of State (DOS), and photographs maintained in the Department of Defense's (DoD) biometric system. State photograph repositories include drivers' licenses, identification cards, and criminal photographs maintained in Departments of Motor Vehicles[6] (DMV) and similar state agencies. In the event that FACE Operations Services searches probe photographs against other federal partner repositories in the future, it will follow the same processes and procedures described in this PIA. The individual memoranda of understanding (MOUs) with any new partners will outline the procedures specific to that relationship.

The FACE Operations Services maintains FCMS, which is an application within the NGI System architecture. This case management system is used to automate the workflow and data management for the FACE Operations Services. Within the FCMS, FACE Operations Services maintains the search requests, which generally include the name of the requesting FBI agent/analyst, the case number, and some biographic information related to the subject of the probe photo, such as name and date of birth. The FCMS documents the details of all work transactions. Information may include the Biometric Images Examiner (BIE)[7] assigned to the case, general comments, dates of entry and modification, dates and types of searches, and disposition of the analysis to include the summary report. Only the probe photographs and limited biographic information about the subjects are maintained in the FCMS; probe photo, likely candidate photographs and associated information are returned to the authorized FBI agent/analyst in a summary report in Sentinel, the FBI's classified case management system.[8] The FCMS also sends a copy of the summary report to the FBI agent/analyst via the email provided in the original request.

Currently, the FBI agent/analyst submits a FR request by loading the information directly onto a secure Facial Recognition Search Request (FRSR) web form in the FCMS. Access to the FCMS for all authorized FBI requesters is through the Law Enforcement Enterprise Portal (LEEP) system. LEEP is another system managed by the FBI's CJIS Division that provides LE agencies, intelligence partners, and criminal justice entities with centralized access to many different resources and services

---

[3] Photographs may also be received via email in the event of technical issues that prevent submission to FCMS. If the FRSR request is taken through email, FACE Operations staff manually enter the photograph and associated information into the FCMS.
[4] Civil photographs retained in the NGI IPS are not available for FR searching.
[5] The NGI System serves as a national criminal history and biometrics repository. It is addressed in separate privacy documentation.
[6] Some state DMVs cannot enter into agreements with the FBI due to state laws that prohibit the use of driver's license photographs for law enforcement purposes.
[7] A BIE is a specially trained examiner of biometric images, such as facial photographs, who has received comprehensive and intensive training in compliance with current government standards.
[8] Sentinel is addressed in separate privacy documentation.

via a single sign-on. Through LEEP, the FACE Operations Services will accept the FRSR forms from FBI agents/analysts in the staging area of the case management system. FBI agents/analysts may also access the FCMS through LEEP via a secure FBI-owned mobile device.

After FACE Operations Services accepts the requests, they forward the requests for comparison against images from the NGI IPS and other federal and state agency photograph repositories. The FACE Operations Services automatically performs a search of the NGI IPS for all requests, and FBI agents/analysts must select any additional searches from the list of other available federal and state agency repositories. A FRSR transaction is constructed within the FCMS containing the probe image and sent electronically to the NGI IPS. The FCMS is not directly connected to any external photograph repositories for FR searching. Rather, the system sends encrypted e-mail requests, via LEEP, to those agencies (e.g., DoD, DOS passports, and state agencies) and results are returned by encrypted e-mail via LEEP. If a search is requested against the DoD repository, the FACE Operations Services triggers the system to send an e-mail containing the probe image to the DoD system, which requests that a search be performed. All requests to search probes against state agencies repositories are queued up and automatically transmitted via encrypted e-mail to specific state agency points-of-contact in accordance with the established MOUs between FBI CJIS Division and the relevant state(s). The FACE Operations Services has direct search access to the Department of State (DOS) Consular Consolidated Database (CCD) visa photograph repository using the Internet via Hypertext Transfer Protocol Security (HTTP) but, at this time, the FCMS is not being used to request this service. FACE Operations Services uploads the probe image to the CCD using both its upload functions and manual entry and then uses the CCD download function to transmit information to FCMS (e.g., downloading the likely candidate report). FACE Operations Services also manually enters some information from CCD to FCMS, such as visa search data. Probe images uploaded to CCD by the FACE Operations Services are not added to the CCD repository.

Automated FR software compares the probe photograph against the photographs in the relevant photograph repository and returns a gallery of photographs to the FACE Operations Services.[9] These photographs are referred to as "candidates" because FR does not constitute positive identification of an individual. The FBI's NGI System is comprised of multiple biometric algorithms. The NGI IPS FR algorithm was purchased as part of the overall NGI System contract effort. As part of the contractual decisions, the FBI CJIS Division leverages the National Institute of Science and Technology (NIST)[10] testing and accuracy results for operational improvements and implementing them as updates to the NGI System. NIST provides critical validation of FBI operational technology, and its biometric algorithm testing provides valuable insight into the accuracy and performance of capabilities of automated biometric matching products.[11]

The FACE Operations Services supplements the FR capability by conducting some text-based searches of FBI systems that do not contain FR capability, such as the FBI's National Data Exchange (N-DEx) System, a CJIS system that maintains records from the criminal justice lifecycle. These text-

[9] The number of candidates returned in a gallery is based on the individual BIE's discretion. A gallery will always be returned, with a maximum of fifty candidates.
[10] NIST is one of the nation's oldest physical science laboratories. Its core competencies include measurement science, rigorous traceability, and development and use of standards. It is part of the Department of Commerce.
[11] The NGI's System's FR algorithm currently ranks as one of the top five most accurate FR algorithms tested by NIST. NIST's Facial Recognition Vendor Test (FRVT) ongoing results are publicly available continuously updated at https://pages.nist.gov/frvt/html/frvt1N.html.

based search requests are initiated over a secure web connection to the relevant system. After a likely candidate has been determined using FR capability, the BIE may conduct a text-based search using biographic data[12] that the FBI agent/analyst submitted with the probe photo. This data may be searched against other FBI and federal databases; however, the BIE will not search any data that was not provided by the FBI agent/analyst. Frequently, no biographic data accompanies the probe photo, and no text-based searches will be performed. If candidate photos are returned using biographic data, the BIE must conduct a comparison and analysis with the probe to determine if the returned candidate photos is a likely match.

Other agency systems containing facial images are owned and managed by the agencies, which have an interest in ensuring accuracy. The FACE Operations Services generally does not have direct access to other agency systems; rather, the probe photograph is sent to the other agencies for automated searching in their systems. For those agencies that do allow direct access, the FACE Operations Services BIE uses a secure logon to conduct FR searches against the agency's web-based system using the probe photo. The probe photograph is not retained by the agency's web-based system. The BIE then performs a manual review on the returned candidate photographs to determine a likely candidate.

For probe photographs that are searched against other state systems, the state agency generally performs the initial comparison and returns candidates to the FACE Operations Services. A trained BIE in the FACE Operations Services then performs manual reviews of the gallery of candidate photographs to determine a likely candidate. If a likely candidate is found, the photograph is returned to the FBI agent/analyst as a lead for further investigation. The FBI agent/analyst is informed that no LE action may be taken solely based on the likely candidate photo. In many instances, no candidate is returned to the FBI agent/analyst.

Both automated FR comparison and a manual analysis are performed to arrive at a likely candidate decision. Differences in an automated FR comparison and a manual review may be described in the following manner: automated FR software uses pattern matching and does not rely on biological or anatomical models of a face or facial features. Instead, the performance of the automated FR software is entirely dependent upon the patterns which the algorithm developer found to be most useful for matching. Automated FR algorithms creates a mathematical template of a face depicted in an image or video (i.e., a "template") and compares that template against other facial image templates to determine the degree of similarity between those facial images. In the manual review, the BIE performs a morphological and/or anthropometric analysis of the candidate photographs. Morphological analysis involves the direct comparison of facial features and requires the BIE to identify similarities and differences in the observed characteristics. These characteristics can represent features common to many individuals (e.g., the overall shape of the nose, eyes, or mouth), while scars, freckles, and moles may also be taken into consideration. Anthropometric analyses rely on explicit measure of landmarks on the face and a comparison of these measurements between the probe photograph and known subjects.

After FRSRs have been fulfilled (whether a most likely candidate or no candidate has been determined), the FCMS will e-mail the FBI agent via LEEP, and the FACE Operations Services BIE

---

[12] Examples of biographic data include, but are not limited to: name, alias, address, height, weight, eye color, driver's license number/personal identification number, date of birth, and social security number.

will continue to upload the generated report to Sentinel for the FBI agent's/analyst's use. Once reviewed by the BIE, candidate photographs will be deleted and will not be retained in the FCMS. A FRSR Summary Report generated from the FCMS is returned to the FBI agent/analyst who submitted the requests via Sentinel. The FRSR Summary Report includes the probe photos and data submitted by the FBI agents/analysts and the results of the FR searches to include either any likely candidate photos determined by the BIE or a no candidates response. The FRSR Summary Report documenting the results, is maintained in the FACE Operations Services investigative case file in Sentinel. The FBI agent/analyst can determine if they want to make this Electronic Communication (EC) part of their own investigative case file.

To access other agencies' systems for FR purposes, the FACE Operations Services enters into a Memorandum of Understanding (MOU) with each agency. The accesses described in these MOUs are authorized by federal and/or state laws that permit the searching of the photograph repositories for LE purposes. These MOUs are implemented with significant information security requirements and privacy obligations. All parties must use secure electronic means to transmit the photographs and any other associated personally identifiable information (PII). The FBI stores photograph images and any associated PII of the likely candidate(s) to the probe photograph in Sentinel, the FBI's case management system. The FBI immediately destroys all other photographs and associated information. The other party to the MOU ensures that only authorized personnel receive and process the photographs sent by the FBI. These agencies are prohibited from the further sharing and/or dissemination of any information associated with the FBI photographs unless required by law. After the FR search has been completed, these agencies are required to destroy all probe photograph images, and any associated data submitted from the FACE Operations Services.

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

Authority	Citation/Reference
Statute	28 United States Code (U.S.C) §§533-4; 18 U.S.C. §3052, 18 U.S.C. §§2721-25.
Executive Order	
Federal regulation	28 Code of Federal Regulations (C.F.R.) 0.85
Agreement, memorandum of understanding, or other documented arrangement	MOUs have been implemented between the FACE Operations Services and several federal and state partners.
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.

FCMS retains request forms, which may contain a variety of PII. The below chart indicates the types of PII that may be found in the system.

(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 and D	Name field is an optional field if known.
Date of birth or age	X	A, B, C and D	Date of birth or age is an optional field if known.
Place of birth	X	A, B, C and D	Place of birth is an optional field if known.
Gender	X	A, B, C and D	Gender is an optional field if known.
Race, ethnicity, or citizenship	X	A, B, C and D	Race, ethnicity, or citizenship is an optional field if known.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C and D	Social Security Number is an optional field if known.
Tax Identification Number (TIN)			
Driver's license	X	A, B, C and D	Driver's license is an optional field if known.
Alien registration number	X	A, B, C and D	Alien registration number is an optional field if known.
Passport number	X	A, B, C and D	Passport number is an optional field if known.
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			

(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
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C and D	

(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
- Video containing biometric data			
- Fingerprints			
- Palm prints			
- Iris image			
- Dental profile			
- Voice recording/signatures			
- Scars, marks, tattoos			
- Vascular scan, e.g., palm or finger vein biometric data			
- DNA profiles			
- Other (specify)			
System admin/audit data:			
- User ID	X	A	
- User passwords/codes			
- IP address	X	A	
- Date/time of access	X	A	
- Queries run	X	A	
- Content of files accessed/reviewed	X	A	
- Contents of files	X	A	
Other (please list the type of info and describe as completely as possible):	X	A	An FBI case file number is used to verify an open case; all other identifying numbers are optional and may or may not be provided by the FBI agent/analyst.

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

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	
Phone		Email			
Other (specify): The FACE Operations Services does not obtain probe or candidate photographs directly from individuals; rather, the probe photographs are submitted by FBI agents/analysts pursuant to their investigatory authority and candidate photographs are provided by federal and state partners pursuant to their legal authorities.					

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

Government sources:					
State, local, tribal		Foreign (identify and provide the international agreement, MOU, or other documented arrangement related to the transfer)			
Other (specify): The FACE Operations Services only accepts probe photographs from within the FBI; however, probe photographs from other DOJ LE components and other federal LE agencies may be accepted in the future.					

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

Section 4: Information Sharing

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

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X			The FACE Operations Services only accepts probe photographs from FBI agents/analysts. FACE Operations Services searches or requests that searches of the probe photographs be performed against photographs in other federal and state systems. The FACE Operations Services receives candidate photographs in response to these searches of other government systems. The candidate photos are then compared to the probe photos. See Section 2 for additional detail.
DOJ Components				

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.**
Federal entities	X			FACE Operations Services searches or requests that searches of the probe photographs be performed against photographs in other federal systems. Federal entities return candidate photographs to FACE Operations Services. See Section 2 for additional detail.
State, local, tribal gov't entities	X			FACE Operations Services searches or requests that searches of the probe photographs be performed against photographs in other state systems. State entities return candidate photographs to FACE Operations Services. See Section 2 for additional detail.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

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

No biometrics are released to the public for "open data" purposes. The biometrics, such as photographs, maintained within the NGI System may be used for FBI research and development purposes in accordance with applicable federal law and regulations. The FBI has a longstanding relationship with 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 biometrics 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 biometrics 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.

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.

With respect to the collection of certain biometrics such as photographs, a person under arrest or the subject of a criminal or national security investigation may have no opportunity or right to refuse the collection of the information. As discussed in Section 2, FACE Operations Services accepts only those photographs collected in compliance with the FBI's investigatory requirements. In the future, if assistance is offered to other LE DOJ components, those photographs must be collected in accordance with the applicable law and policy. FBI agents may collect the photographs in a variety of ways depending on the investigation, but all collection must be lawful, including obtained through consent, pursuant to a warrant, or from a repository that has provided the individual written notice of the photo's use. However, the subject of the photograph is unknown in most instances; therefore, it is not feasible for the FBI agent to provide the subject individual notice. FBI personnel must ensure that their use of FR technology does not unlawfully infringe upon privacy rights and civil liberties, and complies with the U.S. Constitution, federal statutes and regulations, DOJ policies, and FBI policies.

The privacy risks associated with lack of notice to affected individuals about the collection, maintenance, or use of probe photographs 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 has a substantial interest in ensuring the accuracy of information in the system, and in taking action to correct any erroneous information 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, to include the Privacy Act. Title 28 C.F.R., part 16 subpart A, provides general guidance on access to the information in FBI files pursuant to the Freedom of Information Act (FOIA), 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.

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.

Driver's license photos may be shared with law enforcement based on federal and state law. In addition, every relevant MOU between FBI CJIS Division and participating states has been released

pursuant to FOIA.

An individual whose submitted photographs are related to a criminal or national security investigation has no opportunity to refuse the collection of biometrics. Nevertheless, 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, when applicable.

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

Title 28 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. Title 28 C.F.R. 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. However, the FBI maintains exemptions from access and amendment provisions of the Privacy Act for certain records in the NGI System.

Section 6: Maintenance of Privacy and Security Controls

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

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** January 9, 2023, to January 8, 2026. The FCMS operated under the FCMS ATO when developed; however, the FBI determined that, as the FCMS resides as a separate subsystem within the NGI System, the FCMS falls within the NGI System's ATO. A separate FCMS ATO is no longer required. **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** No POAMs related to privacy controls.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:

X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** Confidentiality: high; Integrity: high; Availability: high The NGI System is high across all categories on two grounds. The first is that LE officer safety requires access to this information in a timely and accurate manner. The second is that public privacy requires confidentially be maintained to those members of the user community with need to know for this information. The FCMS resides as a subsystem within the NGI System.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The NGI System is continually monitored at the host and network layer. FISMA policy compliance testing occurs monthly.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** Host operating system logs are consolidated into the CJIS enterprise system audit consolidation and monitored for irregular activities or compliance failures. The NGI System Security Administrator reviews security-related logs on a weekly basis.
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: The FACE Operations Services will be audited on a triennial basis by the CJIS Audit Unit. The audit will be executed in accordance with internal audit procedures and will use the same methodology as used in state audits. The audit will assess the appropriate use of the NGI IPS and evaluate compliance with policy requirements associated with access to the CJIS Division systems and information.
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, LE users and appropriate FBI/contract staff receive security/privacy training as an initial requirement of access to the NGI System, and annually thereafter.

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 FACE Operations Services implements privacy-specific safeguards as controls for protecting the confidentiality of PII. The FACE Operations Services is in compliance with all FBI security policies, including those specific to the NGI System, 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, and (4) utilizing automatic lockout if user inactivity exceeds a specified time frame. The LEEP, which the FACE Operations Services utilizes to access the FCMS, also complies with these guidelines.

Security controls for the FCMS 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 the FCMS.

- **Account Management (AC-02)** –Accounts are monitored for atypical usage such as privilege escalation and excessive invalid logons.
- **Access Enforcement (AC-03)** – Account creation and logical access are managed according to the account management policy. Functional managers request/approve accounts according to this policy. The NGI System and sub-systems, enforce role-based access control for all users.
- **Least Privilege (AC-06)** – Role-based access control is strictly defined, enforced, and documented according to policy.
- **Unsuccessful Logon Attempts (AC-07)** – Invalid logon attempts by a user trigger automated mechanisms to lock and report unsuccessful logon attempts.
- **Security Awareness Training Policy (AT-02) and Security Training (AT-03)** – Outlines the basic security awareness training requirements for information system users.
- **Security Awareness Training (AT-02.E02) –**Addresses "Insider Threat" training and reporting procedures.
- **Audit Review, Analysis, and Reporting (AU-06)** – Automated mechanisms are in place to detect and identify and report suspicious activity which would than trigger supplemental manual processes for review and analysis.
- **Identification and Authentication (Organizational Users) (IA-2)** – The LEEP Directory contains all accounts and individual identities and passes a SAML[13] Assertion to the FCMS. For internal privileged users, unique identities and accounts are contained with NGI Lightweight Directory Access Protocol (LDAP) and require authentication before access to the FCMS is granted.
- **Media Access (PM-2)** – Removable media is restricted to privileged users, strictly enforced, monitored, and audited for unauthorized use. Privileged users are identified and vetted by the system, supervisory special agents, special agents, and information system security officers (ISSOs).
- **Protection of Information at Rest (SC-28)** – FACE Operations Services protects the

[13] Security Assertion Markup Language (SAML) is a framework for exchanging authentication and authorization information. Security typically involves checking the credentials presented by a party for authentication and authorization. *See* https://csrc.nist.gov/glossary/term/security_assertion_markup_language.

confidentiality and integrity of information as the system is hosted within an accredited physical space with significant physical and logical protections on the Enterprise Storage System (ESS).

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

The FCMS data will be retained in accordance with the retention schedule approved by the National Archives and Records Administration (NARA). NARA has approved the destruction of FCMS data when queries, photographs, or log entries (1) are 20 years old, and (2) are no longer needed for analysis, or (3) if 20 years have passed since last activity, whichever is sooner. Audit log data will be deleted/destroyed when 20 years old. The FCMS maintains only probe photographs which are also maintained in Sentinel, the FBI's case management system, and may also be maintained in the NGI System, the FBI's fingerprint and criminal history system, which now includes other biometrics when associated with fingerprints. Both Sentinel and the NGI System have significantly longer retention schedules than the FCMS and would permit retrieval of the probe photographs if needed after deletion from the FCMS.

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 SORN is published at 81 Fed. Reg. 27283 (May 5, 2016); 82 Fed. Reg. 24151, 156 (May 25, 2017); 84 Fed. Reg. 54182 (Oct. 9, 2019).

Section 8: Privacy Risks and Mitigation

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

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

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***

- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.***

The return of most likely candidate photographs to the FBI agent/analyst may result in the potential misidentification of a subject. However, the risk is greatly mitigated by both the automated and manual FR comparison of the probe photograph against the candidate photographs. In many instances, no candidate photographs are returned because none meet a high enough face similarity and quality threshold. When a candidate photograph is returned to an investigator, he/she is clearly informed that the photograph serves only as an investigative lead and may not be used on its own to prove identity. This notice is provided via a printed caveat that is included with the return of the most likely candidate photo. The FBI agent/analyst must consider the candidate photograph in conjunction with all other evidence, such as biographic information, physical evidence, and victim and witness statements.

The searching and retention of probe photographs by the FACE Operations Services presents a privacy risk that the face images of individuals may be searched for improper purposes. This risk is mitigated because the probe photographs must be obtained pursuant to the AGG-DOM, the FBI DIOG, the Privacy Act of 1974, and all relevant laws and policies. In other words, the FBI agent/analyst who is requesting the FR search has already met the legal requirements to investigate the subject of the probe photo. The investigative actions taken by the FBI are subject to significant oversight and compliance, exercised both within the FBI and by external entities. On occasion, probe photographs provided to the FACE Operations Services may be associated with a wanted or missing person whose case has become "cold" or administratively closed. The FBI may re-open closed cases with new information or developments, such as leads generated from FR technology. The Face Operations Services will ensure that any future FR activities performed in support of other federal agencies comports with the relevant investigative authorities for the FBI and those other agencies. Although probe photographs are retained in the FCMS, the FACE Operations Services merely retains copies of the same photographs that are maintained by the FBI agent/analysts in Sentinel.

In addition, the searching and retention of the probe photographs by the FACE Operations Services also presents privacy risks that the face images will be disseminated for unauthorized purposes or to unauthorized recipients, or that there will be improper access to the photographs. These risks are mitigated in several ways. For example, the FACE Operations Services personnel receive significant system security and privacy training. In addition, the FACE Operations Services follows stringent physical and system security requirements to ensure that none of the data is lost or compromised. The FCMS maintains documentation of the work transactions conducted by the FACE Operations Services and the System Administrator can audit who logs on, when, and from what terminal, as well as additions, edits, and deletions. The records contained with the FCMS are generally available only to employees of the FACE Operations Services and the FBI agents/analysts who require the information in the furtherance of their investigations. Information could also be provided to 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).

The BIE searches the probe photographs against FBI databases and searches remotely those federal and state FR systems to which direct access has been granted. In most instances, the BIE must send the probe photographs via LEEP to other federal and state agencies to perform FR searching. These searches are conducted pursuant to MOUs that ensure the privacy and security of the information as it travels to and from the FBI and in accordance with federal and state laws. The probe photographs are handled by select FR personnel at the partner agencies. All probe photographs and text associated with the probe photograph request may be maintained in accordance with state and federal laws once the search has been completed and the responses returned to the FACE Operations Services via LEEP email. FBI requests may be logged pursuant to applicable state and federal law. The completed MOUs contain informational, security, and privacy requirements to ensure that the probe photographs and associated information are not subject to unauthorized disclosure of other data breach. The terms of the completed MOUs also reflect that the FBI does not permit the probe photographs to be searched against FR databases that have not received comprehensive legal and policy review and approval both within the FBI and at the external agency.

Access to the FCMS is controlled through user identification (i.e., user ID and password) and authentication procedures. Processes are in place to ensure that only authorized users have access to the database and the information is verified through audit logs. User activity may be audited by system administrators. Every member of the FACE Operations Services has undergone privacy, security, classification, and investigatory training to ensure that information is properly handled. Frequent and random compliancy checks are performed by Supervisory BIEs to ensure that all policies are followed.

In addition, other disclaimers in the FRSR staging area include the notification that the user is accessing a U.S. Government information system which includes the computer being used, the computer network, all computers connected to the network, and any/or storage media attached to the network or to a computer on the network. The information system is provided for U.S. Government-authorized use only and unauthorized or improper use of this system 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. Any communications transmitted through, or data stored on the information system may be disclosed or used for ay U.S. Government-authorized purpose. Furthermore, users are reminded that the use of publicly accessible computers (e.g., libraries, airports, cafes, hotels) to access this information system is unauthorized.

With the FACE Operations Services, 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 information technology 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 CJIS Information Assurance Unit (CIAU) is responsible for ensuring that mechanisms are in place to make certain that individuals are held accountable for implementing these controls adequately and that the controls are functioning as intended. Through the Security Assessment and Authorization (SAA) process and through the system lifecycle, the CIAU and FACE Operations Services together

provide oversight and accountability for the implementation of key controls, specifically those related to the information system security and privacy compliance.