Federal Bureau of Investigation

Privacy Impact Assessment
for the
Facial Analysis, Comparison, and Evaluation (FACE) Phase II System

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: July 9, 2018

(May 2015 DOJ PIA Form)

EXECUTIVE SUMMARY

This Privacy Impact Assessment (PIA) is an update to the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit PIA issued in May 2015.[1] The FACE Services Unit provides automated searching and manual review of investigative photos collected by FBI personnel against authorized photo repositories collected by the FBI and other government agencies. The FBI's Criminal Justice Information Services (CJIS) Division is developing a new case management system for the FACE Services Unit. The scope, process, and workflow of the FACE Services Unit remain essentially the same; however, the FACE Phase II System will provide improved consolidation and efficiency. The FACE Services Unit will use the new FACE Phase II System as an automated work flow management tool to document the details of all work transactions and to process and communicate face recognition requests.

Section 1: Description of the Information System

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

The FACE Services Unit provides investigative lead support to FBI Field Offices, Operational Divisions, and Legal Attaches by comparing the face images of persons associated with open FBI assessments[2] and investigations[3] against face images available in state and federal face recognition systems. In limited instances, the FACE Services Unit provides face recognition support for closed FBI cases (e.g., missing and wanted persons). The FACE Services Unit requires an open assessment or investigation in accordance with the Attorney General's Guidelines for Domestic FBI Operations (AGG-DOM) and the Domestic Investigations and Operations Guide (DIOG) to ensure that the photos have been obtained in compliance with law and policy. The FACE Services Unit provides unique and significant assistance to FBI personnel that cannot be accomplished by other investigative methods.

At this time, the FACE Services Unit offers its support and expertise only within the FBI. In the future, face recognition support may be offered to other law enforcement components within the Department of Justice and/or to other law enforcement federal partners. If so, the FACE Services Unit will follow the same requirements and processes described in this PIA for those officers and agents.

---

[1] See https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments

[2] 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. Assessments cannot be based solely on the exercise of First Amendment protected activities or the race, ethnicity, national origin, or religion of the subject.

[3] 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 security threat activity.

(b) The type of information collected, maintained, used, or disseminated by the system.

In its support of FBI agents and analysts, the FACE Services Unit accepts unclassified photos of subjects of, and persons relevant to, open FBI cases. These photos are called "probe photos." Upon receipt of a probe photo, the FACE Services Unit uses face recognition software to compare the probe photo against photos contained within government photo systems. The FACE Services Unit does not search probe photos against any private, public, or non-governmental photo system. Federal photo repositories include the criminal mugshots in the FBI's Next Generation Identification (NGI) system, the visa and passport photos maintained by the Department of State (DOS), and photos in the Department of Defense's biometric system. State photo repositories include drivers' licenses, identification cards, and criminal photos maintained in Departments of Motor Vehicles (DMV) and similar state agencies.

In order to access other agencies' systems for face recognition purposes, the FACE Services Unit enters into Memoranda of Understanding (MOU) with each agency. These MOUs are authorized by federal and/or state laws that permit the searching of the photo repositories for law enforcement purposes. These MOUs are implemented with significant information security requirements and privacy obligations that are more fully described in the May 2015 PIA.

The FACE Services Unit currently maintains a manual work log hosted on FBINET, an internal classified FBI system. This work log was described in the PIA issued in May 2015.[4] In this work log, the FACE Services Unit 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 work log also serves as a manual workflow management tool for the FACE Services Unit and documents the details of all work transactions. Information may include the Biometric Images Specialist (BIS)[5] assigned to the case, general comments, dates of entry and modification, dates and types of searches, and disposition of the analysis. Only the probe photos and limited biographic information about the subjects are maintained in the work log; most likely candidate photos and associated information are returned to the authorized FBI agent/analyst via Sentinel, the FBI's classified case management system.

After the implementation of the FACE Phase II System, the majority of the FACE Services Unit's automated work flow and data management will be transitioned to the new FACE Phase II System. The FACE Phase II System will capture the same information as the current work log; however, the FACE Phase II System will be a major application within the NGI system architecture. The FACE Phase II System work log will maintain the same information regarding the search requests and workflow transactions as described above.

---

[4] There is no system known as "FACE Phase I." The FBI facial recognition effort that preceded the development of FACE Phase II was this work log described in the May, 2015, PIA.

[5] A Biometric Images Specialist is a specially trained examiner of biometric images, such as facial photos, who has received comprehensive and intensive training in compliance with current government standards.

(c) The way the system operates to achieve the purpose.

The FACE Services Unit generally does not have direct access to other agency systems; rather, the probe photo is sent to the other agency for automated searching in its system. Automated face recognition (AFR) software compares the probe photo against the photos in the relevant photo repository and returns a gallery of photos to the FACE Services Unit. These photos are referred to as "candidates" because face recognition does not constitute positive identification of an individual. For probe photos that are searched against state systems, the state agency generally performs the initial comparison and returns candidates to the FACE Services Unit. A trained BIS in the FACE Services Unit then performs manual reviews of the gallery of candidate photos to determine a most likely candidate. If a most likely candidate is found, the photo is returned to the FBI agent/analyst as a lead for further investigation. The FBI agent/analyst is informed that no law enforcement action may be taken solely on the basis of the most likely candidate photo. In many instances, no candidate is returned to the FBI agent/analyst.

As explained above, both AFR comparison and a manual analysis is performed to arrive at a most likely candidate decision. Differences in an AFR comparison and a manual review may be described in the following manner: AFR software uses pattern matching and does not rely on biological or anatomical models of a face or facial features. Instead, the performance of the AFR software is entirely dependent upon the patterns which the algorithm developer found to be most useful for matching. AFR algorithms create a template from the face which is then compared against other face templates. In the manual review, the BIS performs a morphological and/or anthropometric analysis of the candidate photos. Morphological analysis involves the direct comparison of facial features, and requires the BIS 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 the explicit measure of landmarks on the face and a comparison of these measurements between the probe photo and known subjects.

(d) Who has access to information in the system.

Access to the FACE Phase II System will be limited to the FACE Services Unit staff, authorized CJIS personnel, and authorized FBI personnel who require access to the information or specific areas of the system for performance of their official duties.

(e) How information in the system is retrieved by the user.

Currently, the FACE Services Unit receives the requests for face recognition searches via classified or unclassified e-mail. With the FACE Phase II System, the FBI agent/analyst will submit the face recognition request by loading the information directly onto a secure Facial Recognition Search Request (FRSR) web form in the FACE Phase II System. Access to the FACE Phase II System for all authorized FBI requesters will be through the Law Enforcement Enterprise Portal (LEEP) system. LEEP is another system managed by the FBI's CJIS Division that provides law enforcement agencies, intelligence partners, and criminal justice entities with centralized access to many different resources

and services via a single sign-on. Through LEEP, the FACE Services Unit will accept the FRSR forms from FBI agents/analysts in the staging area of the FACE Phase II System.

(f) How information is transmitted to and from the system.

After the requests have been accepted by the FACE Services Unit, they will be forwarded to the case management part of the FACE Phase II System for comparison against images from the NGI Interstate Photo System (IPS) and other photo repositories. The FACE Services Unit performs a search of the NGI IPS for all requests. A search request transaction is constructed within the FACE Phase II System containing the probe image and sent electronically to the NGI IPS. The FACE Phase II System is NOT directly connected to any external photo repositories for face recognition searching. Rather, the system sends encrypted e-mail requests, via LEEP, to those agencies (e.g., DoD and state DMVs) and results are returned via encrypted e-mail via LEEP. If a search is requested against the DoD repository, the FACE Services Unit 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 DMVs are queued up and automatically transmitted via e-mail to specific DMV points-of-contract in accordance with the established MOUs between CJIS and the relevant state(s). The FACE Services Unit also conducts face recognition searches against the DOS photo repositories but, at this time, the FACE Phase II System is not being used to request these services.

After search requests have been fulfilled (whether a most likely candidate or no candidate has been determined) the FACE Phase II System will e-mail the FBI agent via LEEP and the FACE Services Unit will continue to upload the generated report to Sentinel for the FBI agent's/analyst's use. Once reviewed by the BIS, candidate photos will be deleted and will not be retained in the FACE Phase II System. As with the current work log, the FACE Phase II System will retain only the probe photos submitted by the FBI agents/analysts. The probe photos and most likely candidate photos are maintained in the investigative case file in Sentinel.

The FACE Services Unit supplements face recognition capability by conducting some text-based searches of systems that do not contain face recognition 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-based search requests are initiated over a secure web connection to the relevant system. After a most likely candidate has been determined using face recognition capability, the BIS may conduct a text-based search using biographic data[6] that the FBI agent/analyst submitted with the probe photo. This data may be searched against other FBI and federal databases; however, the BIS 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.

[6] 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.

(g) Whether it is a stand-alone system or interconnects with other systems.

As discussed above, the FACE Phase II System permits FBI user access and electronic communications with external agencies via the LEEP system. As a subsystem of NGI, it also launches face recognition searches of the NGI IPS; however, the system is not linked or connected to any other system, including any photo repository.

(h) Whether it is a general support system, major application, or other type of system.

The FACE Phase II System is an unclassified subsystem that will be a major application located within the NGI system[7] architecture.

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

General personal data					
Name	X	Date of birth	X	Religion	
Maiden name	X	Place of birth	X	Financial info	
Alias	X	Home address	X	Medical information	
Gender	X	Telephone number		Military service	
Age	X	Email address		Physical characteristics	X
Race/ethnicity	X	Education		Mother's maiden name	
Other general personal data (specify): When the FBI agent/analyst submits a probe photo, he/she may provide any known information regarding the subject; however, often even the name of the subject is not known. None of the information is required or necessary to conduct a face recognition search.					

[7] See NGI System of Records Notice at 81 Fed. Reg. 29,284 (May 5, 2016).

Work-related data					
Occupation		Telephone number		Salary	
Job title		Email address		Work history	
Work address		Business associates			
Other work-related data (specify):					

Distinguishing features/Biometrics					
Fingerprints		Photos	X	DNA profiles	
Palm prints		Scars, marks, tattoos	X	Retina/iris scans	
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	X	Queries run	X	Contents of files	X
Other system/audit data (specify):					

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		Hard copy: mail/fax		Online	
Telephone		Email			
Other (specify): The FACE Services Unit does not obtain probe or candidate photos directly from individuals; rather, the probe photos are submitted by FBI agents/analysts pursuant to their investigatory authority and candidate photos are provided by state and federal partners pursuant to their legal authorities.					

Government sources					
Within the Component	X	Other DOJ components		Other federal entities	
State, local, tribal		Foreign			
Other (specify): The FACE Services Unit only accepts probe photos from within the FBI; however, probe photos from other DOJ law enforcement components and other federal law enforcement agencies may be accepted in the future.					

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.)

The searching and retention of probe photos by the FACE Services Unit presents a privacy risk that the face images of individuals may be searched for improper purposes. This risk is mitigated because the probe photos have been obtained pursuant to the AGG-DOM, the DIOG, the Privacy Act of 1974, and all relevant laws and policies. In other words, the FBI agent or FBI analyst who is requesting the face recognition 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 photos provided to the FACE Services Unit 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 face recognition technology. The FACE Services Unit will ensure that any future face recognition activities performed in support of other federal agencies comports with the relevant investigative authorities for the FBI and those other agencies. Also, although probe photos are retained in the FACE Services Unit's work logs, the Unit merely retains copies of the same photos that are maintained by the FBI agents/analysts in Sentinel.

The searching and retention of the probe photos by the FACE Services Unit 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 photos or misuse of the photos. These risks are mitigated in several ways. For example, the FACE Services Unit personnel receive significant system security and privacy training. In addition, the FACE Services Unit follows stringent physical and system security requirements to ensure that none of the data is lost or compromised. The current work log and the FACE Phase II System maintain documentation of the work transactions conducted by the FACE Services Unit and the System Administrator can audit who logs on, when, and from what terminal, as

well as additions, edits, and deletions.

The BIS searches the probe photos against FBI databases and also searches remotely those federal and state face recognition systems to which direct access has been granted. In most instances, the BIS must send the probe photos via LEEP to other state and federal agencies to perform face recognition 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 state and federal laws. The probe photos are handled by select face recognition personnel at the partner agencies. Generally,[8] all photos and text associated with the probe photo request and the candidate galleries are immediately and permanently destroyed by these state and federal agencies once the searches are completed and the responses returned to the FACE Services Unit via the LEEP e-mail. As reflected in the terms of the MOU, the FBI does not permit the probe photos to be searched against face recognition databases that have not received comprehensive legal and policy review and approval both within the FBI and also at the external agency.

Finally, the return of most likely candidate photos 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 face recognition comparison of the probe photo against the candidate photos. In many instances, no candidate photos are returned because none meet a high enough face similarity and quality threshold. When a candidate photo is returned to an investigator, he/she is clearly informed that the photo 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 photo in conjunction with all other evidence, such as biographic information, physical evidence, and victim and witness statements.

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
X	For intelligence activities		For administrative matters
X	To conduct analysis concerning subjects of investigative or other interest		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		
	Other (specify):		

[8] To accommodate certain states that have auditing and/or logging requirements that necessitate retention of probe photos and candidate galleries, the FBI constructs MOUs in compliance with these requirements while also requiring state maintenance of only the minimum information necessary, for the shortest time period necessary, and notification to the FBI of any potential or actual breach of that information.

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 that authority, the FACE Services Unit provides investigative lead support to FBI personnel by comparing face images of subjects who are the focus of active investigations and assessments, and some administratively closed/unresolved investigations. By using face recognition technology to search probe photos against photo repositories, the FACE Services Unit provides unique and specialized value to the FBI's mission to fight crime and terrorism. In many instances, face recognition results in information that is not available with other investigative methods. Candidate photos are used by FBI agents/analysts as leads for a variety of reasons, including further investigation of a potential subject, to determine the identity of a subject already in custody, to discover an alias that the subject may be using, to locate associates of the subject, and to eliminate potential subjects.

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; 18 U.S.C. §3052
	Executive Order	
X	Federal Regulation	28 CFR 0.85
X	Memorandum of Understanding/agreement	MOUs have been implemented between the CJIS Division and several states and federal partners.
	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.)

The FACE Phase II System data will be retained in accordance with the retention schedule approved by the National Archives and Records Administration (NARA) for the FACE Services Unit. The published NARA records schedule number is DAA-0065-2015-0004. NARA has approved the destruction of work log data when queries, photos, or log entries are (1) 20 years old, (2) are no longer needed for analysis, or (3) if 20 years have passed since last activity. The

FACE Phase II System maintains only the probe photos which are also maintained in Sentinel and which also may be maintained in a sequestered file in NGI. Both Sentinel and the NGI System have significantly longer retention schedules than the FACE Phase II System and would permit retrieval of the probe photos if needed after deletion from the FACE Phase II System.

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.]

Both the current work log and the FACE Phase II System are limited to authorized users who are assigned to work within the FACE Services Unit and who possess accounts within the application. Users are further restricted to only those areas allowed by their assigned roles. Server/database access is limited to the application and privileged user accounts on an "as-required" basis for development and maintenance purposes. Moreover, both the current work log and the FACE Phase II System serve as an added level of privacy risk mitigation, as they put users on notice that their activities, including the searching and disseminating of photos, are being recorded and are subject to audit. The FACE Phase II System users have been trained to minimize the use, collection, and retention of personally identifiable information (PII) to what is strictly necessary to accomplish their business purpose and mission. The FACE Phase II System will be subject to extensive security protections, access limitations, and quality control standards. Privileged access to the system is controlled through user identification and multi-factor authentication procedures. Processes are in place to ensure that only authorized users have access to data and is verified through audit logs. User activity is audited by system administrators on a routine and event-driven basis. Every member of the FACE Services Unit has undergone privacy, security, classification, and investigatory training to ensure that information is properly handled. Frequent and random compliance checks are performed by the unit's supervisors to ensure that all policies are followed.

PII Confidentiality Risk Level: ☐ **Low** ☑ **Moderate** ☐ **High**

Access controls

X	Access Enforcement: the system employs role-based access controls. There is no ability to access underlying database without the front-end interface.
N/A	Separation of Duties: users of de-identified PII data are not also in roles that permit access to PII.
X	Least Privilege: user roles enforce the most restrictive set of rights/roles for each user group.
X	Remote Access: remote access is prohibited or limited to encrypted communication channels.
X	User-Based Collaboration and Information Sharing: automated mechanisms are in place for matching access authorizations to contractual/MOU/MOA restrictions.

N/A	Access Control for Mobile Devices: No mobile devices are used for system access.

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.

Identification and Authentication controls

X	Identification and Authentication: users are uniquely identified before accessing PII; remote access requires 2-factor authentication and 30-minute "time-out" functionality.

Media controls

X	Media Access: access to system media (CDs, USB flash drives, backup tapes) is restricted.
X	Media Marking: media containing PII is labeled.
X	Media Storage: media containing PII is securely stored.
X	Media Transport: media is encrypted and stored in a locked container during transport.
X	Media Sanitation: media is sanitized prior to re-use

Data Confidentiality controls

X	Transmission Confidentiality: information is encrypted prior to transmission
X	Protection of Information at Rest: information stored on a secondary storage device (hard drive or backup tape is encrypted.

Information System Monitoring

X	Information System Monitoring: network boundaries are automatically monitored for unusual or suspicious transfers or events

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	X			
Public				
Private sector				

Foreign governments				
Foreign entities				
Other (specify):				

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 records contained with the FACE Phase II System are generally available only to employees of the FACE Services Unit 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). FBI personnel are informed by numerous disclaimers in the FRSR staging area that candidate photos are intended for lead purposes only, and require further investigation. The disclaimer states "The information returned in response to this request is provided as an INVESTIGATIVE LEAD ONLY and is NOT to be considered as a positive identification". Probe photos are sent to state and federal partners in order to compare the probe photos against their respective face recognition systems. In these instances, MOUs, which have been negotiated by the FBI, have been implemented and contain strict informational, security, and privacy requirements to ensure that the probe photos and associated information are not subject to unauthorized disclosure or other data breach. The MOUs also require these agencies to delete all probe images and any associated data submitted from the FACE Services Unit after the face recognition search has been completed.

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 any 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.

Within the FACE Services Unit, 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 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 throughout the system lifecycle, the CIAU and FACE Services Unit together provide oversight and accountability for the implementation of key controls, specifically those related to the information system security and privacy compliance.

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.)

	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
	Yes, notice is provided by other means.	Specify how:
X	No, notice is not provided.	Specify why not: Probe photos are collected pursuant to authorized FBI criminal and national security investigations.

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

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

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

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

With respect to the collection of certain biometrics such as photos, 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 1, FACE Services Unit accepts only those photos collected in compliance with the FBI's investigatory requirements. FBI agents may collect the photos in a variety of ways depending on the investigation, but all collection must be lawful. For example, a photo may be retrieved from a public place, with consent, pursuant to a warrant, or from a repository that has provided the individual written notice of the photo's use. In most instances, the subject of the photo is unknown; therefore, it is not feasible for the FBI agent to provide individual notice and obtain consent.

The privacy risks associated with lack of notice to affected individuals about the collection, maintenance, or use of probe photos 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, 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.

Section 6: Information Security

6.1 Indicate all that apply.

X	A security risk assessment has been conducted. The FACE Phase II System has undergone automated and manual security controls testing as part of the Security Assessment and Authorization (SAA process to achieve Authority To Operate (ATO). The most recent Security Impact Assessment (SIA) is dated 2/24/2017. The risk assessment results have been entered into the Security Division (SecD) RiskVision tool and reviewed by the Information Systems Security Officer/Manager (ISSO/M) and the FBI Authorizing Official (AO).	
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: As part of the SAA process, all identified risks for the FACE Phase II System have been adjudicated to record compliance and a Plan of Actions and Milestones (POA&M) for the security controls requiring further mitigation.	
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: The FACE Phase II System has been functionally tested to ensure that no unauthorized access is permitted.	
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: The FACE Phase II System received a three-year ATO as a Major Application of the NGI System on 06/01/2017. The NGI System was most recently accredited in April 2014 with an ATO extension until July 25, 2018.	
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 Services Unit will be audited on a triennial basis by the CJIS Audit Unit (CAU). 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 provisions in their contract binding them under the Privacy Act.	
X	Contractors that have access to the system 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:	
	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. Explanation: No users outside the component are authorized.
		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 FACE Phase II System implements privacy-specific safeguards as controls for protecting the confidentiality of PII. The FACE Services Unit is 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, and (4) utilizing automatic lockout if user inactivity exceeds a specified time frame. The LEEP, which the FACE Services Unit utilizes to access the FACE Services Phase II System, also complies with these guidelines.

Security controls for the FACE Phase II System 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 FACE Phase II System.

- **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.
- **Identification and Authentication (Organizational Users) (IA-2)** - The LEEP Directory contains all accounts and individual identities and passes a SAML Assertion to the FACE Phase II System. For internal privileged users, unique identities and accounts are contained with NGI Lightweight Directory Access Protocol (LDAP) and require authentication before access to the FACE Phase II System is granted.
- **Media Access (MP-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 ISSOs.
- **Protection of Information at Rest (SC-28)** – FACE Services Unit protects the 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).

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); 66 Fed. Reg. 8425 (Jan. 31, 2001); 66 Fed. Reg. 17200 (Mar. 29, 2001); 82 Fed. Reg. 24147 (May 25, 2017). 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/analyst to the FACE Phase II System often include the subject's citizenship status, as this information may assist with the searching of federal databases. However, information in the FACE Phase II System pertaining to U.S. citizens and permanent resident aliens is generally not retrieved based on citizenship; rather, the information is retrieved based on the personal identifiers, including photo images, as described above in Section 1, "Description of the Information System."