United States Government Accountability Office

Report to the Ranking Member, Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, U.S. Senate

May 2016

FACE RECOGNITION TECHNOLOGY

FBI Should Better Ensure Privacy and Accuracy

The electronic version of this report was reposted August 3, 2016 to correct errors related to figure 4.

GAO-16-267

May 2016

FACE RECOGNITION TECHNOLOGY

FBI Should Better Ensure Privacy and Accuracy

GAO Highlights

Highlights of GAO-16-267, a report to the Ranking Member, Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, U.S. Senate

Why GAO Did This Study

Technology advancements have increased the overall accuracy of automated face recognition over the past few decades. According to the FBI, this technology can help law enforcement agencies identify criminals in their investigations.

GAO was asked to review the FBI's use of face recognition technology. This report examines: 1) the FBI's face recognition capabilities; and the extents to which 2) the FBI's use of face recognition adhered to privacy laws and policies and 3) the FBI assessed the accuracy of these capabilities.

To address these questions, GAO reviewed federal privacy laws, FBI policies, operating manuals, and other documentation on its face recognition capability. GAO interviewed officials from the FBI and other federal and two state agencies that coordinate with the FBI on face recognition.

What GAO Recommends

GAO is making six recommendations, including, that the Attorney General determine why PIAs and a SORN were not published as required and implement corrective actions, and for the FBI director to conduct tests to verify that NGI-IPS is accurate and take steps to determine whether systems used by external partners are sufficiently accurate for FBI's use. DOJ agreed with one, partially agreed with two, and disagreed with three of the six recommendations. In response, GAO clarified one recommendation, updated another recommendation, and continues to believe that all six recommendations remain valid as discussed further in this report.

View GAO-16-267. For more information, contact Diana Maurer at (202) 512-9627 or maurerd@gao.gao

What GAO Found

The Department of Justice's (DOJ) Federal Bureau of Investigation (FBI) operates the Next Generation Identification-Interstate Photo System (NGI-IPS)—a face recognition service that allows law enforcement agencies to search a database of over 30 million photos to support criminal investigations. NGI-IPS users include the FBI and selected state and local law enforcement agencies, which can submit search requests to help identify an unknown person using, for example, a photo from a surveillance camera. When a state or local agency submits such a photo, NGI-IPS uses an automated process to return a list of 2 to 50 possible candidate photos from the database, depending on the user's specification. As of December 2015, the FBI has agreements with 7 states to search NGI-IPS, and is working with more states to grant access. In addition to the NGI-IPS, the FBI has an internal unit called Facial Analysis, Comparison and Evaluation (FACE) Services that provides face recognition capabilities, among other things, to support active FBI investigations. FACE Services not only has access to NGI-IPS, but can search or request to search databases owned by the Departments of State and Defense and 16 states, which use their own face recognition systems. Biometric analysts manually review photos before returning at most the top 1 or 2 photos as investigative leads to FBI agents.

DOJ developed a privacy impact assessment (PIA) of NGI-IPS in 2008, as required under the E-Government Act whenever agencies develop technologies that collect personal information. However, the FBI did not update the NGI-IPS PIA in a timely manner when the system underwent significant changes or publish a PIA for FACE Services before that unit began supporting FBI agents. DOJ ultimately approved PIAs for NGI-IPS and FACE Services in September and May 2015, respectively. The timely publishing of PIAs would provide the public with greater assurance that the FBI is evaluating risks to privacy when implementing systems. Similarly, NGI-IPS has been in place since 2011, but DOJ did not publish a System of Records Notice (SORN) that addresses the FBI's use of face recognition capabilities, as required by law, until May 5, 2016, after completion of GAO's review. The timely publishing of a SORN would improve the public's understanding of how NGI uses and protects personal information.

Prior to deploying NGI-IPS, the FBI conducted limited testing to evaluate whether face recognition searches returned matches to persons in the database (the detection rate) within a candidate list of 50, but has not assessed how often errors occur. FBI officials stated that they do not know, and have not tested, the detection rate for candidate list sizes smaller than 50, which users sometimes request from the FBI. By conducting tests to verify that NGI-IPS is accurate for all allowable candidate list sizes, the FBI would have more reasonable assurance that NGI-IPS provides leads that help enhance, rather than hinder, criminal investigations. Additionally, the FBI has not taken steps to determine whether the face recognition systems used by external partners, such as states and federal agencies, are sufficiently accurate for use by FACE Services to support FBI investigations. By taking such steps, the FBI could better ensure the data received from external partners is sufficiently accurate and do not unnecessarily include photos of innocent people as investigative leads.

Contents

Letter		1
	Background	5
	FBI Has a Face Recognition System and Uses External Systems to Support Law Enforcement Investigations	10
	FBI and DOJ Could Improve Transparency and Oversight to Better Safeguard Privacy	18
	FBI Has Limited Information on the Accuracy of its Face Recognition Technology Capabilities	25
	Conclusions	33
	Recommendations for Executive Action	34
	Agency Comments and Our Evaluation	35
Appendix I	Objectives, Scope, and Methodology	41
Appendix II	FBI Face Recognition Summary Statistics	46
Appendix III	States Partnered with FBI's Facial Analysis, Comparison, and Evaluation (FACE) Services Unit	50
Appendix IV	Comments from the Department of Justice	52
Appendix V	GAO Contact and Staff Acknowledgments	62

Tables

Table 1: U.S. Department of Homeland Security Fair Information Practices Principles	9
Table 2: Facial Analysis, Comparison, and Evaluation (FACE) Services' Access to Face Recognition Systems	16
Table 3: Number of Searchable Criminal Photos and Civil Photos Enrolled by State and Federal Agencies in Next Generation Identification-Interstate Photo System (NGI-IPS), as of December 2015	46

Table 4: Number of Photos Available to Facial Analysis, Comparison, and Evaluation (FACE) Services by Repository as of December 2015 47
Table 5: Summary of Facial Analysis, Comparison, and Evaluation (FACE) Services Unit Searches and Photos Retuned to Agents from August 2011 through December 2015 49

Figures

Figure 1: Face Recognition Enrollment and Matching Process 6
Figure 2: Description of the FBI's Face Recognition System Request and Response Process for State and Local Law Enforcement 13
Figure 3: Key Dates in the Implementation of the FBI's Face Recognition Capabilities and Associated Privacy Impact Assessments 20
Figure 4: Information Available for FBI Facial Analysis, Comparison, and Evaluation (FACE) Services' Photo Searches, by State 51

Abbreviations

CJIS	Criminal Justice Information Services Division
DOD	Department of Defense
DOJ	Department of Justice
FACE	Facial Analysis, Comparison, and Evaluation Services
FBI	Federal Bureau of Investigation
IAFIS	Integrated Automated Fingerprint Identification System
IPS	Interstate Photo System
MOU	memorandum of understanding
NGI	Next Generation Identification
OPCL	Office on Privacy and Civil Liberties
PIA	Privacy Impact Assessment
SORN	System of Records Notice
TSA	Transportation Security Administration

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 16, 2016

The Honorable Al Franken
Ranking Member
Subcommittee on Privacy, Technology and the Law
Committee on the Judiciary
United States Senate

Dear Senator Franken:

Of all the technologies used to identify people based on their biological and behavioral characteristics, face recognition most closely mimics how people identify others: by scrutinizing their face. What is an effortless skill in humans has proven difficult to replicate in machines, but computer and technology advancements over the past few decades have increased the overall accuracy of automated face recognition. According to the Federal Bureau of Investigation (FBI), these advancements in face recognition technology can help law enforcement agencies identify criminals in federal, state and local investigations. For example, the FBI and one of its state partners used face recognition in June 2015 to help identify a sex offender who had been a fugitive for nearly 20 years. The FBI's Criminal Justice Information Services (CJIS) Division is responsible for developing and implementing the Bureau's face recognition capabilities, and has spent about $55 million on these efforts since 2010.

As the law enforcement community adopts face recognition technology for investigative purposes, academics and privacy advocates have questioned whether it is sufficiently accurate for this use. In addition, the use of face recognition technology raises concerns regarding the protection of privacy and individual civil liberties. For example, the Electronic Frontier Foundation—a privacy advocate—raised concerns in

2012 that face recognition technology could allow for covert, remote, and mass capture and identification of images.[1]

As we reported in July 2015, for commercial uses of face recognition, federal laws do not fully address key privacy issues such as the circumstances under which the technology may be used.[2] However, several statutory requirements govern the protection of personal information by federal agencies, including the FBI's use of face images. For example, the Privacy Act of 1974 places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records.[3] The Privacy Act requires agencies to publish a notice—known as a System of Records Notice (SORN)—in the Federal Register identifying, among other things, the categories of individuals whose information is in the system of records, and the type of data collected.[4] Also, the E-Government Act of 2002 requires agencies to conduct Privacy Impact Assessments (PIA) that analyze how personal information is collected, stored, shared, and managed in a federal system.[5] Agencies are required to make their PIAs publicly available if practicable.

You asked us to review the FBI's use of face recognition technology. This report addresses the following questions: (1) What are the FBI's face recognition capabilities? (2) To what extent has FBI's use of face recognition adhered to laws and policies related to privacy? (3) To what extent does the FBI assess the accuracy of its face recognition capabilities?

[1]*What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcommittee on Privacy, Technology and the Law of the Senate Committee on the Judiciary*, 112th Cong. 24 (2012) (statement of Jennifer Lynch, Staff Attorney, Electronic Frontier Foundation). The Electronic Frontier Foundation is an advocacy organization that focuses on issues related to privacy, free speech online, surveillance, and technology.

[2]See GAO, *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*, GAO-15-621 (Washington, D.C.: July 30, 2015).

[3]A system of record is defined by the Privacy Act of 1974 as a group of records containing personal information under the control of any agency from which information is retrieved by the name of an individual or by an individual identifier. Pub. L. No. 93-579 (Dec. 31, 1974), as amended; 5 U.S.C. 552a(a)(4)(5).

[4]5 U.S.C. 552a(e)(4)(B).

[5]Sec. 208(b), Pub. L. No. 107-347 (Dec. 17, 2002); 44 U.S.C. 3501 note.

To address the first question, we reviewed FBI documentation describing the FBI's face recognition technology capabilities, including an implementation guide, operating manual, and memorandums of understanding (MOUs) between the FBI and its federal and selected state partners. We reviewed these documents in order to understand, among other things, the FBI's face recognition capabilities used for criminal investigations and how the FBI and its partners conduct face recognition searches. Further, we visited the CJIS facility in West Virginia to observe a demonstration of FBI's face recognition capabilities. To better understand how the FBI coordinates with federal and state partners and how these partners' face recognition databases are populated and maintained, we interviewed Department of State (State), Department of Defense (DOD), Michigan, and Texas officials responsible for coordinating with the FBI's face recognition officials. We selected DOD and State because these are the only federal agencies with face recognition MOUs with the FBI. We selected Michigan and Texas because both states had agreements with the FBI that covered multiple face recognition capabilities.[6]

To address the second question, we identified and reviewed privacy protections under federal law, including the Privacy Act of 1974, the E-Government Act of 2002, and Office of Management and Budget guidance to determine DOJ and FBI statutory responsibilities related to protecting privacy of personal information in the FBI's use of face recognition technology. We reviewed and evaluated DOJ policies and guidance to better understand DOJ's privacy structure and identify its PIA and SORN development and review process.[7] In addition, we analyzed the FBI's published PIAs and SORNs to determine what the FBI has disclosed to the public regarding the personal information collected for its face recognition capabilities and how it uses the data. We assessed the relevant FBI public notices and disclosures published from 1999 through

[6]Michigan, New Mexico, and Texas were the only states that had agreements with the FBI that covered both FBI face recognition capabilities at the time of their selection. Selecting Michigan and Texas offered some geographic dispersion. While these selections are not generalizable to other states, we believe they provide important context into face recognition capabilities at the state level.

[7]Department of Justice (DOJ), DOJ Order 0601: Privacy and Civil Liberties (Washington, D.C.: Feb. 2014); DOJ Office of Privacy and Civil Liberties, Senior Component Official on Privacy Manual, Spring 2014 (Washington, D.C.: June 2014); and DOJ Office of Privacy and Civil Liberties, Privacy Impact Assessments Official Guidance (Washington, D.C: Mar. 2012).

2015 against legal and policy requirements as well as the Fair Information Practice Principles.[8] Further, we analyzed FBI's policies and mechanisms of oversight of its face recognition services concerning privacy, such as audit reports, and compared them to *Standards for Internal Control in the Federal Government* and the Fair Information Practice Principles to determine the extent to which the FBI oversees adherence to its privacy policies.[9]

To address the third question, we assessed the FBI's face recognition test results for accuracy against the testing requirements in the FBI's Information Technology Life Cycle Management Directive and face recognition literature developed by the National Science and Technology Council and the National Institute of Standards and Technology.[10] Further, we compared the FBI's efforts to conduct operational assessments on its face recognition capability to the FBI, DOJ, and Office of Management and Budget guidance—such as the FBI Information Technology Life Cycle Management Directive—and draft testing guidelines established by the Facial Identification Scientific Working Group.[11] Further, we reviewed MOUs between the FBI and external partners to determine the extent to which the MOUs addressed accuracy of the face recognition technologies these partners use and the data they provide to the FBI. We compared the FBI's efforts to assess the accuracy

[8]For purposes of this review, we used the eight Fair Information Practice Principles developed by the U.S. Department of Homeland Security, which are discussed later in this report.

[9]GAO, *Internal Control: Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: Nov. 1999).

[10]See FBI, *FBI Information Technology Life Cycle Management Directive*, version 3.0 (Aug. 19, 2005), DOJ, *Systems Development Life Cycle Guidance* (Jan. 2003), OMB, *Circular No. A-11, Planning, Budgeting, and Acquisition of Capital Assets*, V 3.0 (2015), and National Institute of Standards and Technology, *Face Recognition Vendor Test: NIST Interagency Report 8009* (May 26, 2014) and National Science and Technology Council, *Biometrics Frequently Asked Questions* (Sept. 7, 2006).

[11]Facial Identification Scientific Working Group, draft, *Understanding and Testing for Face Recognition Systems Operation Assurance, version* 1.0 (Washington, D.C.: Aug. 15, 2014). Established by the FBI in 2009, the Facial Identification Scientific Working Group's mission is to develop consensus standards, guidelines, and best practices for the discipline of image-based comparisons of human features, primarily face, as well as to provide recommendations for research and development activities necessary to advance the state of science in this field. Participants include representatives from federal, state, local, and international agencies, as well as scientists, practitioners, and persons from the research and academic communities.

of the face recognition services operated by external partners to *Standards for Internal Controls in the Federal Government*.[12] Further, we assessed these efforts against the Fair Information Practice Principles. To learn more about how the FBI assesses its face recognition capability and the external systems it has access to for accuracy, we interviewed officials from Michigan, Texas, DOD and State.

To address all three objectives, we interviewed DOJ and FBI officials, including FBI Headquarters, CJIS, the FBI's Privacy and Civil Liberties Unit, and DOJ's Office on Privacy and Civil Liberties (OPCL).

We conducted this performance audit from January 2015 to May 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. For more information on our scope and methodology, see appendix I.

Background

How Face Recognition Technology Works

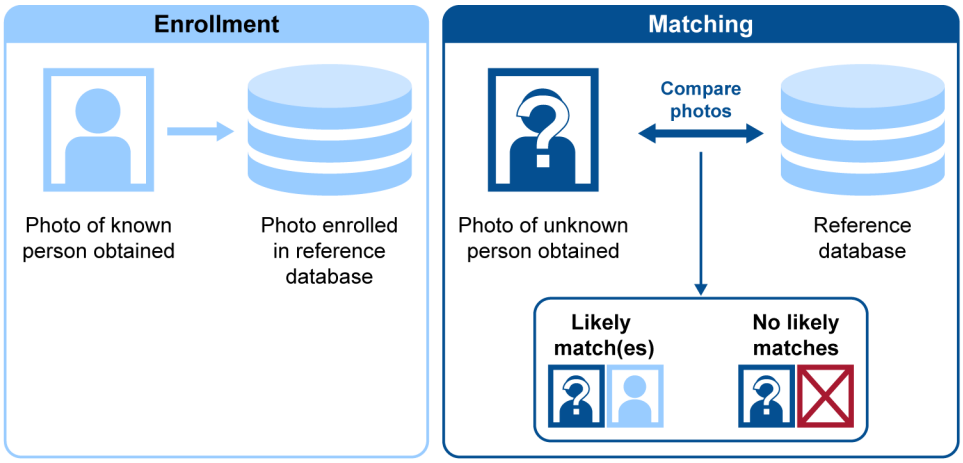
Biometrics is the automated recognition of individuals based on their biological and behavioral characteristics. Technologies have been developed to identify people using biometrics, such as their faces, fingerprints, eye retinas and gait, among other things. Face recognition technology can perform several functions, including the face comparison of an unknown person against a database of known persons.[13] Performing this face comparison generally consists of two processes, an enrollment process and a matching process. During enrollment, a known person's photo is processed by the face recognition technology and stored with biographic information in the reference database of known persons. During matching, a photo of an unknown person (often called a probe photo) is processed by the face recognition technology and

[12]GAO/AIMD-00-21.3.1.

[13]For the purposes of this report, face recognition technology is one component of a face recognition system, which includes hardware, software, and a database of stored images.

compared against all other photos in the database of known persons.[14] If the technology determines that two photos are sufficiently similar, then they will be returned as a likely match. One or more likely matches may be identified and a list of best-matched photos will be generated by the technology, as shown in figure 1. On the other hand, depending on the technology's configuration, the system could return no matches if no photos are found to be sufficiently similar.

Figure 1: Face Recognition Enrollment and Matching Process



Source: GAO analysis of FBI and National Academy of Sciences documentation. | GAO-16-267

Several companies offer face recognition technologies. Because each company has its own proprietary techniques for extracting the distinctive features from a face photo and determining whether two photos are a likely match, the ability of these technologies to accurately perform face comparisons will vary. The accuracy of face recognition systems is often characterized by two metrics – the detection rate (how often the technology generates a match when the person is in the database) and the false positive rate (how often the technology incorrectly generates a match to a person in the database). Matching errors can be caused not

[14]Specifically, the technology extracts features from the faces and puts them into a format—often referred to as a faceprint—that can be used for verification, among other things. Once the faceprint has been created, the technology can use a face recognition algorithm to compare the faceprints against each other to produce a single score value that represents the degree of similarity between the two faces.

only by the quality of a company's face recognition technology, but also by the quality of the photos used in the matching process.

FBI's Use of Biometric Technologies

For decades, fingerprint analysis has been the most widely used biometric technology for positively identifying arrestees and linking them with any previous criminal record. In July 1999, the FBI implemented the Integrated Automated Fingerprint Identification System (IAFIS)—a national, computerized system for storing, comparing, and exchanging fingerprint data in a digital format—which reduced fingerprint submission and processing times from weeks (or longer) to hours. To populate IAFIS, copies of fingerprints taken as a result of an arrest at the local or state level were submitted to the state's central repository, which, in turn, were forwarded to the FBI for entry into IAFIS. Federal arresting law enforcement agencies also captured the fingerprints and personal identifiers of an individual taken into custody and submitted the information to the FBI.

Beginning in 2010, the FBI began incrementally replacing IAFIS with Next Generation Identification (NGI) at an estimated cost of $1.2 billion.[15] NGI was not only to include fingerprint data from IAFIS and biographic data, but also to provide new functionality and improve existing capabilities by incorporating advancements in biometrics, such as face recognition technology. As part of the fourth of six increments, the FBI updated the Interstate Photo System (IPS) to provide a face recognition service that allows law enforcement agencies to search a database of criminal photos that accompanied a fingerprint submission using a probe photo.[16] The FBI began a pilot of NGI-IPS in December 2011, which became fully operational in April 2015.

Privacy Laws and Policies

Federal agency collection and use of personal information, including face images, is governed primarily by two laws: the Privacy Act of 1974[17] and

[15]The FBI expects to complete the last NGI increment by 2017.

[16]When the FBI implemented IAFIS in 1999, CJIS began storing mugshots submitted with fingerprints in a photo database and also digitized all previously submitted hardcopy mugshots. However, until NGI, users could only search for photos using the person's name or unique FBI number.

[17]Pub. L. No. 93-579 (Dec. 31, 1974), as amended; 5 U.S.C. 552a.

the privacy provisions of the E-Government Act of 2002.[18] The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records. The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public through a SORN in the *Federal Register*. According to OMB guidance, the purposes of the notice are to inform the public of the existence of systems of records; the kinds of information maintained; the kinds of individuals on whom information is maintained; the purposes for which they are used; and how individuals can exercise their rights under the Act.[19] Further, the E-Government Act of 2002 requires that agencies conduct PIAs before developing or procuring information technology (or initiating a new collection of information) that collects, maintains, or disseminates personal information. The assessment helps agencies examine the risks and effects on individual privacy and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. OMB guidance also requires agencies to perform and update PIAs as necessary where a system change creates new privacy risks, for example, when the adoption or alteration of business processes results in personal information in government databases being merged, centralized, matched with other databases or otherwise significantly manipulated.[20]

DOJ privacy policies also govern the FBI's use of face recognition technology. For example, it is DOJ's policy to follow the Fair Information Practices Principles, which provide a framework for balancing the need for privacy with other public policy interests, such as national security and law enforcement.[21] The U.S. Department of Homeland Security has

[18]Sec. 208(b), Pub. L. No. 107-347 (Dec. 17, 2002); 44 U.S.C. 3501 note.

[19]OMB, *Privacy Act Implementation: Guidelines and Responsibilities*, 40 FR 28948, 28962 (July 9, 1975).

[20]M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003).

[21]Department of Justice, *Privacy and Civil Liberties*, DOJ Order 0601, Feb. 6, 2014. The Fair Information Practices Principles, which form the basis of the Privacy Act, were first proposed in 1973 by a U.S. government advisory committee as a set of principles for protecting the privacy and security of personal information. Since that time, these have been widely adopted as a benchmark for evaluating the adequacy of privacy protections. The Fair Information Practice Principles are not precise legal requirements.

developed a version of these principles that the FBI's Biometric Center of Excellence references (see table 1).[22]

Table 1: U.S. Department of Homeland Security Fair Information Practices Principles

Principle	Description
Transparency	The department should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personal information.
Individual participation	The department should involve the individual in the process of using personal information, and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of personal information. The department should also provide mechanisms for appropriate access, correction, and redress regarding the use of personal information.
Purpose specification	The department should specifically articulate the authority that permits the collection of personal information and specifically articulate the purpose or purposes for which the personal information is intended to be used.
Data minimization	The department should only collect personal information that is directly relevant and necessary to accomplish the specified purpose(s) and only retain personal information for as long as is necessary to fulfill the specified purpose(s).
Use limitation	The department should use personal information solely for the purpose(s) specified. Sharing personal information outside the department should be for a purpose compatible with the purpose for which the personal information was collected.
Data quality and integrity	The department should, to the extent practicable, ensure that personal information is accurate, relevant, timely, and complete.
Security	The department should protect personal information (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
Accountability and auditing	The department should be accountable for complying with these principles, providing training to all employees and contractors who use personal information, and auditing the actual use of personal information to demonstrate compliance with these principles and all applicable privacy protection requirements.

Source: U.S. Department of Homeland Security| GAO-16-267

Face Recognition Roles and Responsibilities at DOJ

CJIS, the largest division in the FBI, was established in February 1992 to serve as the focal point and central repository for criminal justice information services, which includes responsibility for NGI. CJIS also maintains the FBI's repositories of fingerprints and biographical data and is responsible for implementing the FBI's face recognition capabilities. CJIS' mission is to equip law enforcement, national security, and

[22]U.S. Department of Homeland Security, *The Fair Information Practice Principles*, Privacy Policy Guidance Memorandum Number 2008-01 (Dec. 29, 2008). The Biometric Center of Excellence is the FBI's program for exploring and advancing the use of new and enhanced biometric technologies and capabilities for integration into operations, turning them into effective tools for the law enforcement and intelligence communities.

intelligence community partners with the criminal justice information they need to protect the United States while preserving civil liberties.

Within DOJ, preserving civil liberties and protecting privacy is a shared responsibility by department level offices such as OPCL and components, such as the FBI. For example, while the FBI drafts privacy documentation for its face recognition capabilities, DOJ offices review and approve key documents developed by the FBI—including SORNs and PIAs.

FBI Has a Face Recognition System and Uses External Systems to Support Law Enforcement Investigations

FBI Operates a National Face Recognition System to Support Federal, State, and Local Criminal Investigations

Sources and Enrollment of Photos

FBI's NGI-IPS includes a database of about 30 million photos that is used by selected state law enforcement agencies and the FBI to conduct face recognition searches to support criminal investigations.[23] The majority of photos enrolled in NGI-IPS are voluntary submissions from 18,000 federal, state, local, and tribal law enforcement entities. About 70 percent of the photos in NGI-IPS were criminal mugshots stored in IAFIS that were not searchable with face recognition technology until the development of NGI.[24] According to the *NGI-IPS Policy and Implementation Guide* and FBI officials, NGI-IPS allows law enforcement officials to more efficiently and effectively search photos of missing

[23]The 30 million photos in NGI-IPS represent about 16.9 million individuals.

[24]The remaining photos have been submitted since the development of NGI-IPS.

persons, suspects, or criminals against the criminal mugshots that the FBI has on file.[25] FBI officials said that NGI-IPS has been used by law enforcement officers conducting investigations of credit card and identity fraud, bank robberies, and violent crimes, among others. For example, in July 2014 the FBI compared a suspect's images captured through video surveillance with NGI-IPS criminal mug shots, which provided an investigative lead that helped identify a bank robbery suspect who was ultimately convicted.

According to the NGI-IPS Policy Implementation Guide, to be enrolled in NGI-IPS, all face photos must include a tenprint submission of the individual (submission of all ten fingerprints).[26] The NGI-IPS database has two categories of photos: criminal identities (photos submitted as part of a lawful detention, an arrest, or incarceration), and civil identities (photos submitted for licensing, employment, security clearances, military service, volunteer service, and immigration benefits). Over 80 percent of the photos in NGI-IPS are criminal. According to FBI officials, if more than one photo of the same person exists in the database, these photos are linked by an automated search of NGI using fingerprints when submitted by partner agencies. For example, if an individual has a civil identity in NGI-IPS and the same individual subsequently has a criminal identity established in NGI-IPS because of an arrest, all previously collected biometrics (including civil photos) become associated with the criminal identity file.[27] Any fingerprint data of a person is linked to the entirety of the person's other biometric data in the NGI-IPS database (both criminal and civil), including photos, thereby creating a one identity system. Appendix II provides additional summary statistics on the FBI's face recognition capabilities.

According to FBI officials, local, state and federal agencies voluntarily submit criminal and civil photos for enrollment into NGI-IPS.[28] For

[25]See FBI CJIS Division, *NGI-IPS Policy and Implementation Guide, version 1.2* (Clarksburg, WV: Sept. 3, 2014).

[26]Probe photos used for face recognition searches, such as photos taken from security cameras or social media photos are not enrolled into NGI-IPS.

[27]According to the FBI, should the individual's criminal file be removed (through expungement), the associated civil photo will be returned to the individual's civil file and will no longer be available as a candidate within a search result.

[28]According to the FBI, photo enrollment requirements in the IPS (whether civil or criminal) are based on current law and policy, and only mugshots are permitted for criminal photos.

example, officials in the two states we met with told us that local law enforcement officials are allowed to enroll criminal photos into NGI-IPS at the time suspects are booked for a crime. Additionally, images may be removed from NGI-IPS at the request of the submitting agency, by court order, or if the image is of poor quality. An individual can also request to have their criminal record, including photos, expunged under certain circumstances following procedures in the state where the arrest occurred.

Searching NGI-IPS Using Face Recognition Technology

Local, state, federal, and tribal law enforcement agencies can obtain access to NGI-IPS in order to submit face recognition searches for law enforcement purposes. NGI-IPS only allows users to conduct face recognition searches in the criminal identities part of the database; no searches are permitted in the civil identities part of the database.[29] At the time of our review, the FBI is the only federal agency with direct access to NGI-IPS, and the search process it uses to support active internal investigations is described later in this report. In December 2011, as part of a pilot program, the FBI also began incrementally allowing a limited number of states to submit face recognition searches against a subset of criminal images in the FBI's database—first IAFIS, and then NGI-IPS.[30] Authorized states conducted over 20,000 face recognition searches from December 2011 through December 2015 as part of the pilot.[31] According to FBI officials, in April 2015, the FBI authorized the full operation of NGI-IPS and allowed for the submission of face recognition searches against the full criminal database, rather than just a subset. As of December

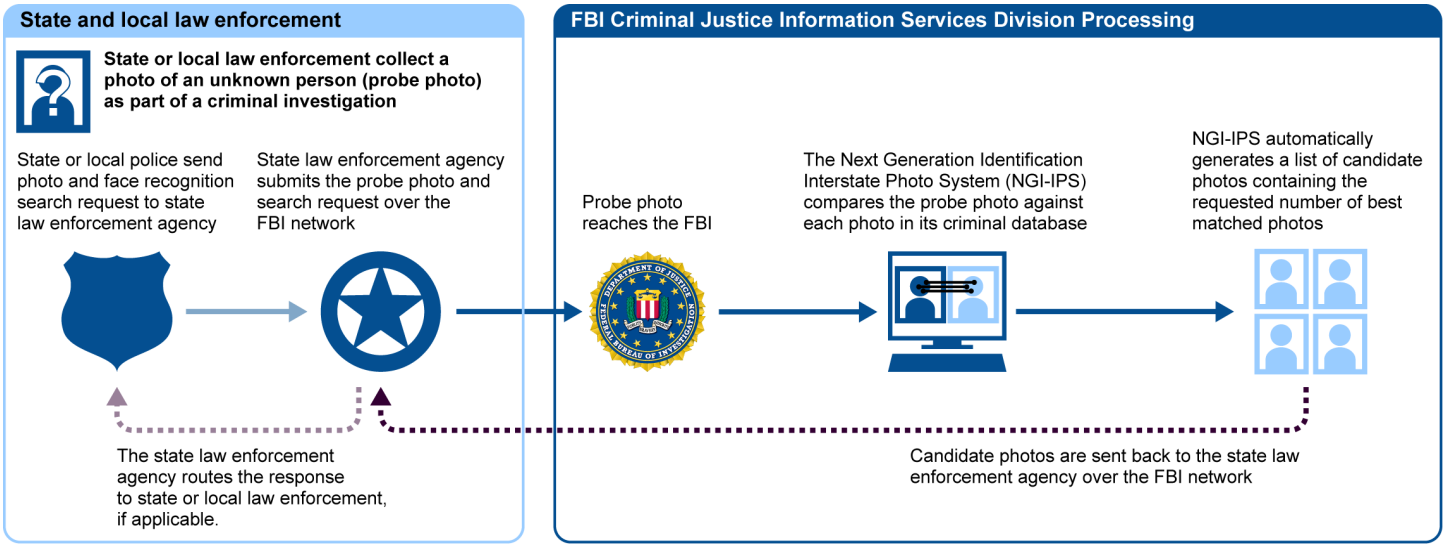
[29]According to FBI officials, the FBI decided not to allow searches of the civil photos enrolled in NGI to better protect individuals' privacy. An additional search capability the FBI is exploring for NGI-IPS is the inclusion of the Unsolved Photo File (UPF). While not enrolled in the civil or criminal databases, the NGI-IPS Policy and Implementation Guide states that authorized law enforcement users, such as states, may place probe photos of an unknown individual that is lawfully obtained as part of an authorized criminal investigation of a felony in a separate part of NGI-IPS, called the unsolved photo file. However, as of August 2015, CJIS has not enabled this feature in NGI-IPS.

[30]Michigan and Maryland signed MOUs with the FBI to participate in the NGI-IPS pilot in 2011, Maine and New Mexico in 2012, Texas in 2013, and Florida in 2014. According to the MOUs for the pilot between participating states and the FBI, the subset of NGI-IPS photos would not represent a real time reflection of the NGI-IPS database, but would be expanded and updated periodically throughout the pilot. FBI officials stated that the subset of photos was updated every Friday.

[31]The FBI did not include civil photos in the pilot database, and, as a result, no searches conducted under the pilot returned civil photos. Beginning in April 2015, states started transitioning from the pilot to full operational capability.

2015, the FBI has agreements with 7 states (Florida, Maryland, Maine, Michigan, New Mexico, Texas, and Arkansas) to submit searches to NGI-IPS and their level of usage has varied.[32] For example, from the beginning of the pilot in December 2011 through December 2015, the number of search requests by states ranged from under 20 by one state to over 14,000 by another state. According to FBI officials, the FBI is working with 8 additional states to grant them access to NGI-IPS for face recognition searches, and an additional 24 states are interested in connecting to NGI-IPS. However, according to the FBI, use of NGI-IPS for face recognition searches is voluntary, and the FBI does not know if the remaining 11 states are interested in connecting to NGI-IPS. Figure 2 describes the process for a search requested by state or local law enforcement.

Figure 2: Description of the FBI's Face Recognition System Request and Response Process for State and Local Law Enforcement



Source: GAO analysis of FBI documentation. | GAO-16-267

As shown in figure 2, to conduct face recognition searches, state and local law enforcement officials submit through their state law enforcement agency a probe photo, such as an Automated Teller Machine camera

[32]Authorized law enforcement users are those with an Originating Agency Identifier designating the user as a law enforcement agency including a unit or subunit of a local, state, federal or tribal government with the principle functions of prevention, detection, and investigation of crime, apprehension of alleged offenders, and enforcement of laws.

photo, pertaining to criminal investigations.[33] NGI-IPS allows law enforcement officials to request between 2 and 50 photos to be returned from a face recognition search, with 20 candidates being the default. These likely matches are called "candidate photos" because they serve only as investigative leads and do not constitute positive identification.[34] For example, officials we interviewed from Michigan stated that they always ask for 50, which is useful when submitting probe photos that are lower quality because results are less accurate and there is a greater chance of the correct match being outside the top 10 or 20 candidate photos.

The search of NGI-IPS is a completely automated process, in which the system compares the probe photo to all enrolled photos in NGI-IPS criminal database without human analysis.[35] The face recognition search is only conducted on images in NGI-IPS's criminal database. However civil photos may be returned in the search of the criminal database if they are linked to a criminal identity record. After NGI-IPS is searched using face recognition technology, the system automatically produces a list containing the requested number of candidate photos in rank order and automatically returns the ranked list of candidate photos for use as investigative leads to the state law enforcement agency.[36] According to the FBI, when the requesting law enforcement agency receives the candidates, human analysis must be performed on all returned images to determine whether the person may be a subject of interest relevant to its investigation.

[33]According to the IPS Policy and Implementation Guide, law enforcement agency electronically submits the request to the FBI using CJIS's network which connects various criminal justice information, such as NGI and the National Crime Information Center, among others. The IPS Policy and Implementation Guide also states that all appropriate use policies must protect the constitutional rights of all persons and should expressly prohibit collection of photos in violation of an individual's 1st and 4th amendment rights.

[34]The term "positive identification" means a determination, based upon a comparison of fingerprints or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record.

[35]Specifically, the system compares the photos using specific data points on the face, such as the distance between the eyes, and calculates a match score—a numerical value representing the similarity between the probe and candidate photo—for each photo enrolled in the NGI-IPS criminal database, and then provides the photos in a rank ordered list.

[36]NGI-IPS will always return the requested number of photos, between 2 and 50, even if none of them are a close match.

FBI Uses NGI-IPS and Various External Face Recognition Systems to Support Internal FBI Investigations

CJIS has a unit called Facial Analysis, Comparison, and Evaluation (FACE) Services that conducts face recognition searches on NGI-IPS and can access external partners' face recognition systems to support FBI active investigations.[37] FACE Services began supporting investigations in August 2011. According to the FACE Services Privacy Impact Assessment, the ability of the FACE Services Unit to leverage information in NGI-IPS and external databases improves the FBI's ability to fight crime and terrorism. Unlike NGI-IPS which primarily contains criminal photos, these external systems primarily contain civil photos from state and federal government databases, such as visa applicant photos and selected states' driver's license photos.[38] There are 29 trained biometric images specialists in FACE Services who receive requests from the FBI field offices, investigative divisions, and FBI overseas offices to support active FBI investigations. When an FBI agent submits a probe photo to FACE Services, a biometric images specialist searches NGI-IPS for matches to the probe photo. However, agents may request that the biometric images specialist also search the face recognition systems of FBI's external partners, as described in table 2.[39] The total number of face photos available in all searchable repositories is over 411 million,

[37]According to the FBI, all probe photos submitted to the FACE Services Unit have been collected pursuant to legal authority. According to the *Privacy Impact Assessment for the FACE Services Unit*, in limited instances, the FACE Services Unit provides face recognition support for closed FBI cases (e.g., missing and wanted persons) and may offer face recognition support to federal agency partners. However, at the time of our review, FBI officials stated that the FBI did not offer this service to other federal agencies.

[38]According to the FBI, the external photo databases do not contain privately obtained photos or photos from social media, and the FBI does not maintain these photos; it only searches against them. Also, according to the FBI, legal authority exists for the face recognition searching of all of these photo databases. For example, the FBI stated that the states are authorized to use the law enforcement exception of the Driver's Privacy Protection Act to permit sharing photos with the FBI. Further, the FBI also has MOUs with their partner agencies that describe the legal authorities that allow the FBI to search the partner agencies' photos.

[39]Although the FBI can access partners' databases to support criminal investigations, these external systems are used by partner agencies for various other purposes. For example, the Department of State uses its face recognition system to help identify fraudulent visa applications, and similarly, individual states use their face recognition systems to help detect fraud in driver's license applications. The Department of Defense's face recognition system is used to support warfighters in the field to identify enemy combatants.

and the FBI is interested in adding additional federal and state face recognition systems to their search capabilities.[40]

Table 2: Facial Analysis, Comparison, and Evaluation (FACE) Services' Access to Face Recognition Systems

Agency Face Recognition System	Description of Content	Method of Obtaining Likely Matches	Number of Likely Matches Returned
FBI's Next Generation Identification - Interstate Photo System	Criminal justice photos that accompanied a fingerprint submission to the FBI	Direct Access	By requested number between 2 and 50
Department of State Face Recognition on Demand[a]	Visa applicant photos.	Direct Access	Up to 88
	Photos from the Terrorist Screening Center database of those known or reasonably suspected of being involved in terrorist activity		
	U.S. citizen passport application photos[b]	Search Requested	Up to three
Department of Defense (DOD)'s Automated Biometric Identification System	A photo repository of, among others, individuals detained by U.S. forces abroad	Search Requested	DOD only returns one photo, if a match is found[c]
16 state face recognition systems	All 16 state databases include driver's license photos, and 4 state databases also include criminal photos	Search Requested	Varies by state[d]

Source: GAO analysis of agency information.| GAO-16-267

[a]According to the Department of State Face Recognition on Demand is used to search the Consular Consolidated Database for visa photos, and also searches the Terrorist Watchlist.

[b]In October 2015, State and the FBI initiated a 180 day pilot for State to conduct face recognition comparisons of persons under FBI investigation against passport photos in the State passport database.

[c]DOD's face recognition system searches face images to generate a score. Photos with scores below a pre-defined threshold are considered to be a no match, and anything above the threshold score is sent for examiner review. Although the Automated Biometric Identification System (ABIS) contains a small number of U.S. citizen photos, those images are not shared with agencies outside DOD.

[d]According to FBI documentation, the number of photos returned to FACE Services by states range from 1 to 50. For more detail on which states partner with FBI for FACE Services requests, see appendix III.

To request a search, the requesting FBI agent sends a probe photo and indicates on a request form which systems the agent would like FACE Services to search in addition to NGI-IPS. As shown in table 2, biometric images specialists have direct access to two face recognition systems

[40]The over 411 million refers to photos, not identities.

and must request searches for the other 18 face recognition systems. Further, for those systems from which searches must be requested, the level of manual review of results by the external party varies. For example, according to FBI officials, at FBI's request, state partners conduct automated searches of their own databases, and some states manually review the automated search results to determine if a likely match exists before selecting photos to return to the FBI. Other states return photos without conducting any manual analysis. The search process conducted by federal partners varies. For example, DOD personnel review the results of the automated face recognition searches that the FBI requests from their system and only return most likely matches to the FBI. Specifically, any candidate photos that DOD's face recognition system matches to the probe photo are reviewed independently by two DOD biometric examiners. If both decide there is a match, DOD provides the FBI biometric images specialist with data regarding the individual, including name and demographic information.[41] If the FBI sends State an automated photo search against visa applicant photos, the automatically generated potential photo matches will be returned to the FBI for review. In the pilot State is running, if the FBI sends State a request for a photo search against U.S. passport photos, State personnel will review the automatically generated potential photo matches and select the most likely photo matches to return to the FBI. FBI then reviews State photos and determines if any are a match to the source photo.

Once results of the searches of NGI-IPS and any other requested databases are returned, the FACE Services biometric images specialist manually reviews the candidate photos and sends the top one or two to the requesting FBI agent as a potential lead.[42] From August 2011 through December 2015, FBI agents have requested almost 215,000 searches of external partners' databases. Of these requests, about 36,000 have included searches on state driver's license databases. Additional information on FACE Services repositories and searches is in appendix II.

[41]FBI biometric images specialists must request the associated photo from DOD after receiving any initial match information.

[42]The request form an FBI agent submits to FACE Services states that any results returned as part of the request is provided as an investigative lead only and is not to be considered a positive identification. Additionally, the FBI stated the agent cannot take any independent law enforcement action based on the photo, meaning the photo is only one part of the full investigation.

According to FBI officials, biometric images specialists respond to the FBI agents who submitted the search request within 24 hours and may send additional photos later if external partners do not provide results within that timeframe. According to FACE Services officials, if biometric images specialists determine that none of the databases returned a likely match, they do not return any photos to the agents.

FBI and DOJ Could Improve Transparency and Oversight to Better Safeguard Privacy

DOJ Has an Oversight Structure in Place to Protect Privacy, but, Until Recently, Had Not Completed Required PIAs

DOJ has an oversight structure in place to help ensure privacy protections, but the FBI did not update the NGI-IPS PIA in a timely manner when the system underwent significant changes or develop and publish a PIA for FACE Services before that unit began supporting FBI agents.

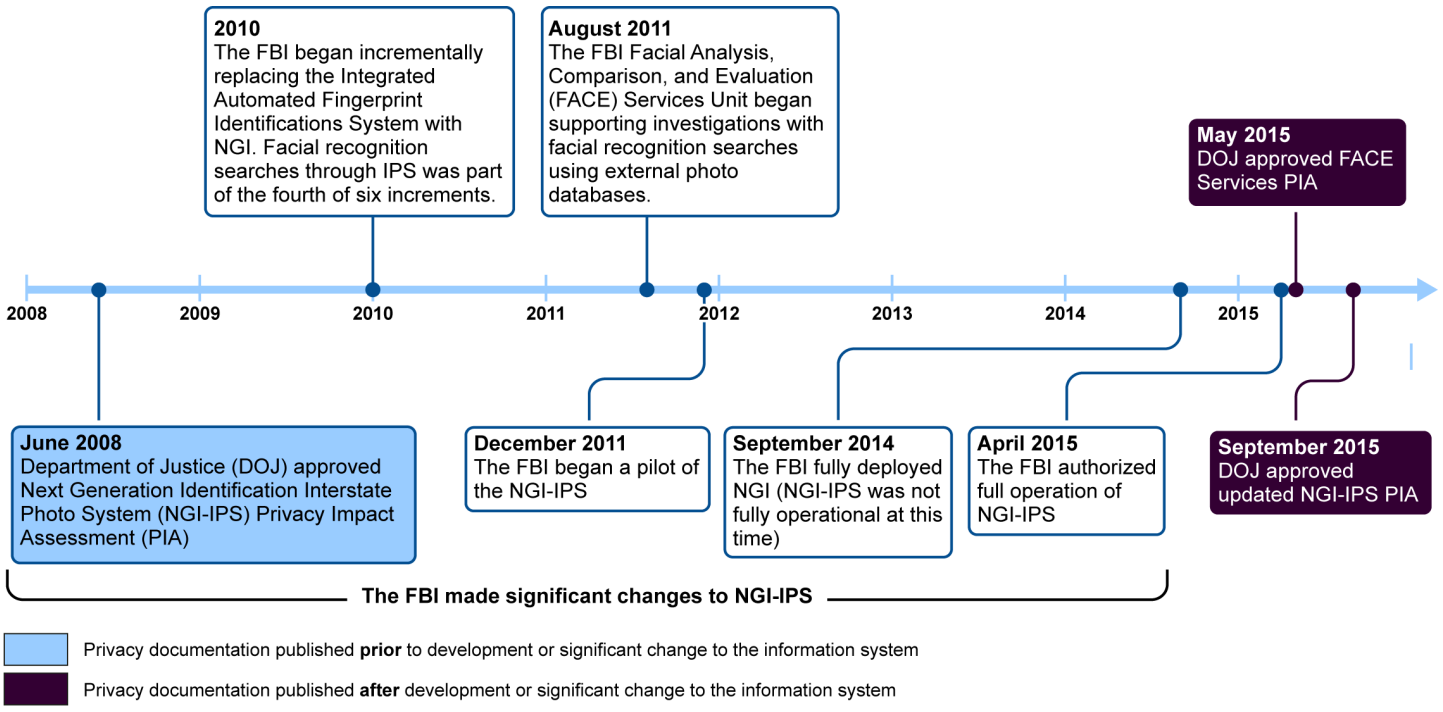
DOJ and the FBI have established oversight structures to help protect privacy and oversee compliance with statutory requirements. For example, by law, the Attorney General appoints a Chief Privacy and Civil Liberties Officer who oversees OPCL and is responsible for reviewing and approving DOJ's SORNs and PIAs to ensure the department's compliance with statutory privacy requirements. OPCL is to coordinate with components in developing their required privacy documentation and provide legal guidance to ensure DOJ's compliance with privacy laws and policies. Accordingly, OPCL established guidance that explains, for example, when DOJ components, including the FBI, should complete their PIAs and SORNs, and the process for developing their PIAs. Within the FBI, the Privacy and Civil Liberties Unit advises program officials throughout implementation of a system or project to ensure that use policies, operating procedures, and required privacy documentation and reports, including PIAs and SORNs reflect privacy and security safeguards. After the FBI completes required privacy documentation, FBI program and privacy officials coordinate with OPCL to review and revise these documents—a process that OPCL officials stated can take months.

Consistent with the E-Government Act and OMB guidance, OPCL developed guidance for DOJ that requires initial PIAs to be completed at

the beginning of development of information systems and anytime there is a significant change to the information system in order to determine whether there are any resulting privacy issues. DOJ published a PIA at the beginning of the development of NGI-IPS, as required. Specifically, in 2008 the FBI published a PIA of its plans for NGI-IPS. However, the FBI did not publish a new PIA or update the 2008 PIA before beginning the NGI-IPS pilot in December 2011 or as significant changes were made to the system through September 2015. In addition, DOJ did not approve a PIA for FACE Services until May 2015—over three years after the unit began supporting FBI agents with face recognition searches.[43] As noted in DOJ guidance, PIAs give the public notice of the department's consideration of privacy from the beginning stages of a system's development throughout the system's life cycle and ensures that privacy protections are built into the system from the start–not after the fact–when they can be far more costly or could affect the viability of the project. Figure 3 provides key dates in the implementation of these face recognition capabilities and the associated PIAs.

[43]The FBI conducted a privacy threshold assessment of FACE Services in 2012 that determined a PIA was necessary for the worklog used to store personal information. According to DOJ guidance, a privacy threshold assessment—now called an initial privacy assessment—is the first step in a process developed by OPCL to assist DOJ components in the development and use of information systems. Specifically, the initial privacy assessment is a tool used to facilitate the identification of potential privacy issues; to assess whether additional privacy documentation is required; and ultimately, to ensure DOJ's compliance with applicable privacy laws and policies.

Figure 3: Key Dates in the Implementation of the FBI's Face Recognition Capabilities and Associated Privacy Impact Assessments



Source: GAO analysis of DOJ and FBI information. | GAO-16-267

According to FBI officials, NGI-IPS was not operational during the pilot because states did not conduct searches against the full criminal database. Further, FBI officials stated that they drafted an updated PIA for NGI-IPS in January 2015 and submitted it to DOJ for review—before NGI-IPS became fully operational in April 2015. These officials also stated that significant changes were made to NGI-IPS only after the FBI had drafted the PIA. Regarding FACE Services, FBI officials stated that legal guidance was provided to FACE Services since the unit's inception and privacy protections were incorporated into every practice of the unit. In addition, FBI officials stated that the PIAs were written as program decisions were being determined, that the PIA drafting was an integral part of program development, and that PIAs are published to reflect years of decision making.

However, the FBI made significant changes to NGI-IPS after publishing the 2008 PIA and used the system to conduct over 20,000 searches to assist in investigations throughout the pilot. For example, the 2008 PIA states that NGI-IPS is in the study phase, which includes the

development of functional and system requirements. However, in December 2011, the FBI implemented the NGI-IPS pilot, which constitutes a significant change in the FBI's use of the technology. Further, the 2008 PIA identified IAFIS as a major supporting system of NGI-IPS in the 2008 PIA, but NGI replaced IAFIS in September 2014. According to FBI officials, the change from IAFIS was one of the reasons the FBI determined an updated PIA was needed. As a result, DOJ/FBI was required by the E-Government Act and OMB guidance to update the PIA as changes were made to NGI-IPS from 2011 through 2015.

Similarly, DOJ/FBI has acknowledged that FACE Services began supporting FBI investigations in 2011, which involved storing photos in a new work log and also performing automated searches instead of manual searches. As a new use of information technology involving the handling of personal information, it too, required a PIA. During the course of our review, DOJ approved the NGI-IPS PIA in September 2015 and the FACE Services PIA in May 2015. DOJ and FBI officials stated that these PIAs reflect the current operation of NGI-IPS and FACE Services.

Standards for Internal Control in the Federal Government calls for federal agencies to compare actual performance to planned or expected results throughout the organization and analyze significant differences.[44] Moreover, according to the E-Government Act, as well as OMB and DOJ guidance, PIAs are to be assessments performed before developing or procuring such technologies and upon significant system changes. However, as the internal drafts of these PIAs were updated, the public remained unaware of the department's consideration for privacy throughout development of NGI-IPS and FACE Services because the updates were not published, as required. Specifically, delays in the development and publishing of up-to-date PIAs for NGI-IPS and FACE Services limited the public's knowledge of how the FBI uses personal information in the face recognition search process. By addressing the PIA development process, DOJ would more closely adhere to DOJ guidance and could help ensure the timely development and publishing of PIAs to increase transparency of the department's systems and missions, thereby providing the public with greater assurance that DOJ components are evaluating risks to privacy when implementing systems.

[44]GAO/AIMD-00-21.3.1.

DOJ Did Not Complete a SORN Addressing FBI's Face Recognition Capabilities in a Timely Manner

Prior to completion of our review, DOJ had not published a SORN that addresses the collection and maintenance of photos accessed and used through the FBI's face recognition capabilities. OPCL provides guidance and advises DOJ components, including the FBI, on whether a particular information system or holding of personal information qualifies as a system of record and whether it is necessary to draft a new SORN, or to modify an existing SORN. OPCL officials stated that NGI is considered to be a system of records as defined by the Privacy Act, and is covered by the SORN that FBI has in place for the FBI's Fingerprint Identification Record System, which discusses fingerprint searches. However, at the time of our review, the existing version of the SORN, dated September 1999, did not address the collection and maintenance of photos accessed and used through NGI for the FBI's face recognition capabilities. According to DOJ officials, OPCL determined that the fingerprint SORN was legally sufficient because it made reference to "related criminal justice information," which OPCL interpreted to implicitly include the photos used in NGI's face recognition capabilities. Nonetheless, during our review, OPCL officials told us they were in the process of drafting a new SORN for NGI in an effort to enhance transparency by explicitly describing NGI's new technologies, including automated face recognition searches. On May 5, 2016—after completion of our review—the FBI published a notice of the modification of the Fingerprint Identification Records System to be renamed the Next Generation Identification (NGI) System.

While the new SORN addresses face recognition, those capabilities have been in place since 2011. Throughout this period, the agency collected and maintained personal information for these capabilities without the required explanation of what information it is collecting or how it is used. According to OPCL officials, the FBI initially waited to complete the NGI SORN until all of NGI's capabilities were identified in order to provide a comprehensive explanation of NGI and limit the number of necessary SORN revisions. FBI officials added that they met regularly with OPCL to complete the SORN. SORNs are a mechanism to increase transparency of the personal information collected by government agencies. Consistent with the transparency Fair Information Practice Principle, the Privacy Act of 1974 requires that when agencies maintain a system of records a SORN must be published in the Federal Register "upon" the establishment or revision of the system of records.[45] According to OMB

[45]5 U.S.C. 552a(e)(4).

guidance, the SORN "must appear in the Federal Register before the agency begins to operate the system, e.g., collect and use the information."[46] Completing and publishing SORNs in a timely manner is critical to providing transparency to the public about the personal information agencies plan to collect and how they plan to use the information. By assessing the SORN development process and taking corrective actions to ensure timely development of future SORNs, DOJ would provide the public with greater understanding of how their personal information is being used and protected by DOJ components.

FBI Has Not Completed Audits to Oversee the Use of NGI-IPS or FACE Services

CJIS has established an audit program to evaluate compliance with restrictions on access to CJIS systems and information by its users, such as the use of fingerprint records, but it has not completed audits of the use of NGI-IPS or FACE Services searches of external databases.

Consistent with the Fair Information Practice Principles, the FBI has specified the purpose and use of NGI-IPS and FACE Services in their user policies and agreements. CJIS policy states that it is the responsibility of the CJIS system users—such as states and local law enforcement agencies—to develop usage policies for NGI-IPS, which should expressly prohibit collection of photos in violation of an individual's First and Fourth Amendment rights. Further, CJIS Security Policy states that the CJIS Audit Unit is required to conduct triennial audits of each of its state and local law enforcement users, to assess agency compliance with applicable statutes, regulations, and policies related to CJIS systems.[47] In accordance with its policy, the CJIS Audit Unit has conducted triennial National Identity Services audits of CJIS system users to assess their compliance with federal laws and regulations when accessing CJIS databases.[48] However, while these audits have examined certain information accessed by NGI users they have not yet assessed the use of face recognition searches of NGI-IPS. FBI officials also told us that NGI-IPS has not been operational long enough to undergo an audit.

[46]OMB Circular A-130, App. I, sec. 5.a(2)(a) (2000).

[47]Department of Justice, *Criminal Justice Information Services Security Policy*, Version 5.3, CJISD-ITS-DOC-08140-5.3, Aug. 2014.

[48]Specifically, the CJIS Audit Unit conducts the National Identity Services audit to assess compliance with federal laws and regulations associated with the use, dissemination, and security of criminal history record information, among other things.

However, state and local users have been accessing NGI-IPS since December 2011 and have generated IPS transaction records since then that would enable CJIS to assess user compliance.[49] For example, by reviewing transaction records, CJIS could assess the reasons law enforcement users submitted face recognition searches and determine the extent to which their use was authorized. According to CJIS officials, they developed a draft audit plan in summer 2015 that includes the review of NGI-IPS transaction records, and they expect it to be finalized after a review by the Advisory Policy Board in the spring of 2016.[50] The FBI did not provide us with any documentation of the draft audit plan.

In addition, as described earlier, the FACE Services Unit has been using external databases that include primarily civil photos to support FBI investigations since August 2011, but the FBI has not audited its use of these databases. According to CJIS Audit Unit officials, they could conduct a minimally-scoped review of the FACE Services Unit's use of external databases, but it does not have the primary authority or obligation to audit such use—which is the responsibility of the owners of the databases. Further, according to these officials, the CJIS Audit Unit's mission and function center on the integrity and security of CJIS systems, not of the FBI's use of data from external systems. We understand the FBI may not have authority to audit the maintenance or operation of databases owned and managed by other agencies. However, the FBI does have a responsibility to oversee the use of the information by its employees. According to the FACE Services PIA, the searching and retention of probe photos by the FACE Services Unit presents privacy risks that the facial 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. The PIA further states that the FACE Services work log captures information identifying the user, as well as the user's activities, including dates and types of searches conducted and the disposition of the FACE Services analysis. Reviewing this information as part of a periodic audit would help the FBI to ensure

[49]Transaction records are a log of communications between CJIS and CJIS system users. NGI-IPS transaction records would include, among other things, tenprint submissions transactions, images submissions for an existing identity, face recognition search requests, and face image search results.

[50]The FBI's Advisory Policy Board is responsible for reviewing appropriate policy, technical, and operational issues related to the FBI's Criminal Justice Information Services Division programs.

compliance with FBI privacy policies and, therefore, better safeguard privacy protections.

Standards for Internal Control in the Federal Government calls for federal agencies to design and implement control activities to enforce management's directives and to monitor the effectiveness of those controls.[51] The Fair Information Practice Principles also state that agencies should audit the actual use of personal information to demonstrate compliance with all applicable privacy protection requirements. Without conducting audits to determine the extent to which users are conducting facial image searches in accordance with CJIS policy requirements, the FBI cannot be sure that FBI officials are implementing CJIS' face recognition capabilities in accordance with privacy policy requirements.

FBI Has Limited Information on the Accuracy of its Face Recognition Technology Capabilities

FBI Has Conducted Limited Assessments of the Accuracy of NGI-IPS Face Recognition Searches

Pre-deployment Testing

Prior to accepting and deploying NGI-IPS, the FBI conducted testing to evaluate how accurately face recognition searches returned matches to persons in the database, but the tests were limited because they did not include all possible candidate list sizes and did not specify how often incorrect matches were returned. Specifically, the FBI established a

[51] GAO/AIMD-00-21.3.1.

detection rate requirement for face recognition searches in the NGI System Requirements Document that states when the person exists in the database, NGI-IPS shall return a match of this person at least 85 percent of the time (the detection rate). Prior to accepting and deploying the NGI-IPS system, FBI tested the detection rate using predefined test cases on a known data set consisting of 926,000 photos. According to NGI-IPS testing documents, the system met the detection rate requirement because 86 percent of the time, a match to a person in the database was correctly returned within a candidate list of 50 potential matches. FBI officials told us that they perform the same controlled testing when NGI-IPS undergoes any significant changes—such as when the company that provides the FBI with the face recognition technology updates that technology—to help ensure that the system's accuracy is the same or better before deploying the update in the operational environment. These officials stated that using a controlled, constant database provides a useful baseline when conducting subsequent tests.

Although the FBI has tested the detection rate for a candidate list of 50 photos, NGI-IPS users are able to request smaller candidate lists—specifically between 2 and 50 photos. FBI officials stated that they do not know, and have not tested, the detection rate for other candidate list sizes. According to these officials, a smaller candidate list would likely lower the detection rate because a smaller candidate list may not contain a likely match that would be present in a larger candidate list. According to a Texas Department of Safety official responsible for coordinating with the FBI on the state's NGI-IPS searches, Texas law enforcement officials request different candidate list sizes when submitting search requests, sometimes less than 50 photos. According to the FBI Information Technology Life Cycle Management Directive, testing needs to confirm the system meets all user requirements. Because the accuracy of NGI-IPS's face recognition searches when returning fewer than 50 photos in a candidate list is unknown, the FBI is limited in understanding whether the results are accurate enough to meet NGI-IPS users' needs.

Further, FBI officials stated that they have not assessed how often NGI-IPS face recognition searches erroneously match a person to the database (the false positive rate). The FBI initially established a 20 percent false positive rate in the NGI System Requirements Document. However, according to our review of NGI-IPS testing and acquisition documents, the FBI decided that the false positive requirement was not relevant when NGI-IPS was returning a candidate list of 50 potential matches, and therefore did not test the requirement. FBI officials stated that NGI-IPS returns a ranked list of candidates that law enforcement

officials who requested the search must analyze to determine if any of candidates have value as an investigative lead. Therefore, according to FBI officials, because the results are not intended to serve as positive identifications, the false positive rate requirement is not relevant.

However, according to the National Science and Technology Council and the National Institute of Standards and Technology, the detection rate and the false positive rate are both necessary to assess the accuracy of a face recognition system. Following the same methods used by the National Institute of Standards and Technology, the FBI could test the false positive rate with the detection rate test using the same test database. Generally, face recognition systems can be configured to allow for a greater or lesser number of matches; a greater number of matches would generally increase the detection rate, but would also increase the false positive rate. Similarly, a lesser number of matches would decrease the false positive rate, but would also decrease the detection rate. Reporting a detection rate of 86 percent without reporting the accompanying false positive rate presents an incomplete view of the system's accuracy. According to FBI officials, the system was designed to a specific false positive rate and its system was built to meet that false positive rate, but no testing was performed to validate that the false positive rate was achieved. In addition, the FBI's Information Technology Life Cycle Management Directive states that the FBI must develop requirements for any technology acquisitions and test the system for those requirements periodically. Further, the Fair Information Practice Principles state that personal information, which includes photos, should be accurate and relevant to the purpose for which it is collected.

Given that the accuracy of a system can have a significant impact on individual privacy and civil liberties as well as law enforcement workload, it is essential that both the detection rate and the false positive rate for all allowable candidate list sizes are assessed prior to the deployment of the system. Conducting such accuracy tests prior to accepting and deploying subsequent changes to the system would help ensure that the system is capable of producing sufficiently accurate search results. Specifically, according to a July 2012 Electronic Frontier Foundation hearing statement, false positives can alter the traditional presumption of innocence in criminal cases by placing more of a burden on the defendant

to show he is not who the system identifies him to be.[52] The Electronic Frontier Foundation argues that this is true even if a face recognition system such as NGI-IPS provides several matches instead of one, because each of the potentially innocent individuals identified could be brought in for questioning. In addition, if false positives are returned at a higher than acceptable rate, law enforcement users may waste time and resources pursuing unnecessary investigative leads. By conducting tests to verify that NGI-IPS is sufficiently accurate for all allowable candidate list sizes—including ensuring that the detection and false positive rates are identified—the FBI would have reasonable assurance that NGI-IPS provides investigative leads that help enhance, rather than hinder or overly burden, criminal investigation work. Even more, the FBI would help ensure that it is sufficiently protecting the privacy and civil liberties of U.S. citizens enrolled in the database.

Operational Reviews

The FBI, Department of Justice, and Office of Management and Budget guidance all require annual reviews of operational information technology systems to assess their ability to continue to meet cost and performance goals.[53] For example, the FBI's Information Technology Life Cycle Management Directive requires an annual operational review to ensure that the fielded system is continuing to support its intended mission and can be continuously supported, operated and maintained in the future in a cost effective manner. According to the directive, the emphasis of the operations and maintenance phase is to ensure that the user's needs are met and the system continues to perform as specified in the operational environment. Similarly, the Department of Justice's Systems Development Life Cycle Guidance Document requires an annual review to determine if the system's performance—such as its accuracy—is meeting the user's satisfaction. Further, the Face Identification Scientific Working Group—a working group chaired by the FBI—has developed draft guidelines and techniques to help administrators of automated face

[52]*What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcommittee on Privacy, Technology and the Law of the Senate Committee on the Judiciary*, 112th Cong. 24 (2012) (statement of Jennifer Lynch, Staff Attorney, Electronic Frontier Foundation).

[53]See FBI, *FBI Information Technology Life Cycle Management Directive*, version 3.0 (August 19, 2005); DOJ, *Systems Development Life Cycle Guidance* (Jan. 2003); and OMB, *Circular No. A-11, Planning, Budgeting, and Acquisition of Capital Assets*, V 3.0 (2015).

recognition systems assess their system in an operational setting to provide assurance of face recognition accuracy.[54]

FBI officials have not conducted an operational review of NGI-IPS. As a result, they have not assessed the accuracy of face recognition searches of NGI-IPS in its operational setting—the setting in which enrolled photos, rather than a test database of photos—are used to conduct a search for investigative leads. According to FBI officials, the database of photos used in its tests is representative of the photos in NGI-IPS, and ongoing testing in a simulated environment is adequate. However, according to the National Institute of Standards and Technology, as the size of a photo database increases, the accuracy of face recognition searches performed on that database can decrease due to lookalike faces.[55] FBI's test database contains 926,000 photos while NGI-IPS contains about 30 million photos.

FBI officials would, by conducting an operational review, obtain information regarding what factors affect the accuracy of the face recognition searches, such as the quality of the photos in the database, and if NGI-IPS is meeting federal, state, and local law enforcement needs. In November 2013, we reported on the extent to which federal information technology investments have undergone operational assessments and concluded that until agencies ensure their operational investments are assessed, there is a risk that they will not know whether they are fully meeting intended objectives.[56] By conducting an annual operational review that includes an assessment of the accuracy of face recognition searches on the NGI-IPS system—such as by testing the accuracy rate of searches conducted against photos in the operational NGI-IPS database, or by asking state and local law enforcement if they are satisfied with the results they are getting from NGI-IPS—FBI officials decrease the risk of spending resources on a system that is not operating

[54]Face Identification Scientific Working Group, *Understanding and Testing for Face Recognition Systems Operation Assurance, version* 1.0 (Aug. 15, 2014).

[55]National Institute of Standards and Technology, *Face Recognition Vendor Test: NIST Interagency Report 8009* (May 26, 2014).

[56]GAO, *Information Technology: Agencies Need to Strengthen Oversight of Multibillion Dollar Investments in Operations and Maintenance*, GAO-14-66 (Washington, D.C.: Nov. 6, 2013).

as intended or does not meet law enforcement user needs, and they are better positioned to take steps to improve the system, as needed.

FBI Has Not Assessed the Accuracy of the External Face Recognition Systems Used by FACE Services

FBI officials do not ensure that the accuracy of the face recognition systems operated by external partners is sufficient for use by FACE Services. For example, FBI officials did not establish accuracy requirements for external systems to be used by FACE Services. Further, FBI officials did not assess the accuracy of the external face recognition systems before agreeing to conduct searches on, or receive search results from, these systems. Both Michigan and Texas officials stated that the FBI has not inquired about the accuracy of their states' face recognition system, which FBI officials confirmed.

FBI officials provided several reasons why they do not take additional steps beyond the MOUs to assess the accuracy of their partners' face recognition systems.[57] First, according to FBI officials, their external partners are responsible for ensuring the accuracy of their own face recognition systems and are best positioned to make this evaluation. Further, these partners have their own missions that face recognition help them accomplish, and they have a vested interest in deploying accurate systems. However, states generally use their face recognition systems to prevent a person from fraudulently obtaining a drivers' license under a false name, while the FBI uses face recognition to help identify, among other people, criminals for active FBI investigations.[58] Accuracy requirements for criminal investigative purposes may be different. In addition, other federal government agencies assess the reliability of the data they receive from external partners. For example, as we have reported, the Transportation Security Administration (TSA) has assessed the accuracy and completeness of historical passenger data provided by air carriers for TSA's Secure Flight automated name-matching process.

[57]The FACE Services MOUs between the FBI and state partners include, among other things, the authorities authorizing the sharing of information between the parties, specific responsibilities of the parties, and privacy and security safeguards.

[58]We reported in 2012 that 41 states and the District of Columbia use face recognition technology to detect fraud in driver's license applications by ensuring an applicant does not obtain a license by using the identity of another individual and has not previously obtained licenses using a different identity or identities. See GAO, *Driver's License Security: Federal Leadership Needed to Address Remaining Vulnerabilities*, GAO-12-893 (Washington, D.C.: Sept. 21, 2012).

TSA uses this name-matching process to compare potential matches of passengers against federal government watch lists to determine if they pose a security risk.[59]

In addition, FBI officials also told us that they do not assess the face recognition systems used by external partners because there are a limited number of companies that offer face recognition technology, which the National Institute of Standards and Technology regularly tests for accuracy. However, the specific technology used can affect accuracy. For example, the National Institute of Standards and Technology's 2014 Face Recognition Vendor Test assessed various companies' face recognition technologies and found that some face recognition technologies were less accurate than others.[60] The version of the technology deployed also affects accuracy, as older versions of face recognition technologies are less accurate than newer versions, according to the 2014 Face Recognition Vendor Test. One state official we spoke with told us he made a similar observation. Specifically, the official said that the state has purchased one update to its face recognition system in the 7 years since their original acquisition, and the update—purchased about 4 years ago—noticeably improved the accuracy of the searches. Moreover, as discussed above, accuracy rates of face recognition technologies may be different in a test setting than an operational setting, where other factors—such as the quality of the face photos in the database—can affect accuracy. As a result, FBI partners using the same face recognition technology could have different error rates.

Because the FBI does not assess the accuracy of its partners' technology, it risks relying on technologies that could potentially have higher error rates or could be obsolete. According to FBI officials, they would rather receive data from all available face recognition systems because receiving a valuable investigative lead from an inaccurate system, even if it is infrequent, outweighs the cost of reviewing candidate

[59]GAO, *Aviation Security: Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program*, GAO-06-374T (Washington, D.C.: Feb. 9, 2006).

[60]Specifically, the report stated that error rates can range from a few percent up to beyond fifty percent, depending on the technology. Further, the institute does not test all companies that offer face recognition technology, and participation is voluntary. See National Institute of Standards and Technology, *Face Recognition Vendor Test: NIST Interagency Report 8009* (May 26, 2014).

lists from these systems that do not contain any likely matches (i.e., the candidate list does not contain any useful leads). These officials further stated that they mitigate accuracy risks of external databases by using biometric images specialists to review any photos generated by these databases before providing the results to the FBI agent who requested the search and by providing a caveat with results returned to FBI agents that they are receiving investigative leads. While these actions would help mitigate against face recognition systems with high false positive rates, they do not help with systems with low detection rates. A face recognition system with a low detection rate may not sufficiently provide biometric images specialists with matches when they exist in the partner's system (i.e., the person in the probe photo has a photo in the partner system, but it is not returned as part of the candidate list). As a result, the FBI could miss investigative leads that could have been revealed if the partner system had a better detection rate.

Standards for Internal Controls in the Federal Government calls for agencies to design and implement components of operations to ensure they meet the agencies mission, goals, and objectives, which, in this case, is to identify missing persons, wanted persons, suspects, or criminals for active FBI investigations. By relying on its external partners' face recognition systems, the FBI is using these systems as a component of its routine operations and is therefore responsible for ensuring the systems will help meet FBI's mission, goals and objectives. Further, according to the Fair Information Practice Principles, data quality—including the accuracy of the data—is an important aspect to protecting privacy. The FBI has entered into agreements to search and access external databases—including millions of U.S. citizens' drivers' license and passport photos—but until FBI officials can assure themselves that the data they receive from external partners are reasonably accurate and reliable, it is unclear whether such agreements are beneficial to the FBI and do not unnecessarily include photos of innocent people as investigative leads. By assessing whether each external face recognition system used by FACE Services is sufficiently accurate for its use, the FBI would have better assurance that the systems are helping the bureau to identify potential suspects in its active investigations while protecting privacy. Such an assessment could include, for example, information from the National Institute of Standards and Technology or a review of how external partners determine if such technologies are sufficiently accurate for their own use. It could also include information on any accuracy assessments conducted by these partners—such as accuracy tests states conduct by comparing probe photos to their drivers' license database.

Conclusions

The use of face recognition technology raises potential concerns regarding both the effectiveness of the technology in aiding law enforcement investigations and the protection of privacy and individual civil liberties. As reflected in DOJ guidance, the timely development and publishing of PIAs would increase transparency of the department's systems and missions and provide the public with greater assurance that DOJ components are evaluating risks to privacy when implementing systems. DOJ could accomplish this by (1) assessing the PIA development process to determine why PIAs were not published prior to using or updating face recognition capabilities, and (2) implementing corrective actions to ensure the timely development, updating, and publishing of PIAs before using or making changes to a system.

In addition, without an updated SORN that addresses the FBI's collection and maintenance of photos accessed and used through the FBI's face recognition technology, the public had limited understanding of the nature of the system and how their personal information, including face images, is being used and protected. Further, without conducting audits to determine whether users are conducting face image searches in accordance with CJIS policy requirements, FBI officials cannot be sure they are implementing face recognition capabilities in a manner that protects individuals' privacy.

The FBI is also required to test the accuracy of its technology systems, including NGI-IPS. By conducting tests to verify that NGI-IPS is accurate for all allowable candidate list sizes—including ensuring that the detection and false positive rates are identified—the FBI would have more reasonable assurance that NGI-IPS provides leads that help enhance rather than hinder or overly burden criminal investigation work. Because the FBI does not conduct operational reviews that would assess the accuracy of face recognition searches on NGI-IPS, it risks spending resources on a system that is not operating as intended and also may miss opportunities for improving the system. Also, by taking steps to assess whether the systems operated by external partners are sufficiently accurate for use by FACE Services (i.e., reviewing any accuracy assessments performed by external partners on their own systems), the FBI would have better assurance that the systems they use are appropriate for its use, increasing the odds of identifying suspects for active investigations while protecting privacy.

Recommendations for Executive Action

To improve transparency and better ensure that face recognition capabilities are being used in accordance with privacy protection laws and policy requirements, we recommend that the Attorney General:

- Assess the PIA development process to determine why PIAs were not published prior to using or updating face recognition capabilities, and implement corrective actions to ensure the timely development, updating, and publishing of PIAs before using or making changes to a system.

- Assess the SORN development process to determine why a SORN was not published that addressed the collection and maintenance of photos accessed and used through NGI for the FBI's face recognition capabilities prior to using NGI-IPS, and implement corrective actions to ensure SORNs are published before systems become operational.

To better ensure that face recognition capabilities are being used in accordance with privacy protection laws and policy requirements, we recommend that the Director of the Federal Bureau of Investigation conduct audits to determine the extent to which users of NGI-IPS and biometric images specialists in FACE Services are conducting face image searches in accordance with CJIS policy requirements.

To better ensure that face recognition systems are sufficiently accurate, we recommend that the Director of the Federal Bureau of Investigation take the following three actions:

- Conduct tests of NGI-IPS to verify that the system is sufficiently accurate for all allowable candidate list sizes, and ensure that the detection and false positive rate used in the tests are identified.

- Conduct an operational review of NGI-IPS at least annually that includes an assessment of the accuracy of face recognition searches to determine if it is meeting federal, state, and local law enforcement needs and take actions, as necessary, to improve the system.

- Take steps to determine whether each external face recognition system used by FACE Services is sufficiently accurate for the FBI's use and whether results from those systems should be used to support FBI investigations.

Agency Comments and Our Evaluation

We provided a draft of this report to DOJ, DOD and State for their review and comment. DOD and State did not have formal comments on our draft report but provided technical comments, which we incorporated as appropriate. DOJ provided formal, written comments, which are reproduced in full in appendix IV. DOJ concurred with one and partially agreed with two of our six recommendations, and described actions underway or planned to address them. DOJ did not concur with three recommendations in the report.

DOJ did not concur with our recommendation that DOJ assess the PIA development process to determine why PIAs were not published prior to using or updating face recognition capabilities. DOJ stated that the FBI has established practices that protect privacy and civil liberties beyond the requirements of the law. Further, DOJ stated that it developed PIAs for both FACE Services and NGI-IPS, as well as other privacy documentation, throughout the development of the these capabilities that reflect privacy choices made during their implementation. For example, DOJ stated that it revised the FACE Services PIA as decisions were made. DOJ also stated that it will internally evaluate the PIA process as part of the Department's overall commitment to improving its processes, not in response to our recommendation.

We agree that, during the course of our review, DOJ published PIAs for both FACE Services and NGI-IPS. However, as noted in the report, according to the E-Government Act and OMB and DOJ guidance, PIAs are to be assessments performed before developing or procuring technologies and upon significant system changes. Further, DOJ guidance states that PIAs give the public notice of the department's consideration of privacy from the beginning stages of a system's development throughout the system's life cycle and ensures that privacy protections are built into the system from the start–not after the fact–when they can be far more costly or could affect the viability of the project. As noted in the report, although DOJ published an NGI-IPS PIA in 2008, it did not publish a new PIA or update the 2008 PIA before beginning the NGI-IPS pilot in December 2011 or as significant changes were made to the system through September 2015. In addition, DOJ approved a PIA for FACE Services over three years after the unit began supporting FBI agents with face recognition searches. DOJ stated that it updated these PIAs throughout the development of the FBI's face recognition capabilities. However, as the internal drafts of these PIAs were updated, the public remained unaware of the department's consideration for privacy because the PIA updates were not published, as required. The timely development and publishing of future PIAs would increase

transparency of the department's systems and missions and provide the public with greater assurance that DOJ components are evaluating risks to privacy when implementing systems.

DOJ agreed in part with our recommendation that DOJ complete a SORN for the NGI system that addresses the collection and maintenance of photos accessed and used through the FBI's face recognition capabilities. DOJ stated that it submitted the SORN for publication to the Federal Register on April 21, 2016, and it was published on May 5, 2016. Further, DOJ stated that the NGI-IPS and FACE Services PIAs, not the NGI SORN, represent the best resource for the public to learn about how face recognition technology is used. Specifically, DOJ stated that SORNs are primarily used as a legal notice document, while a PIA is an analysis of how personal information is processed to, among other things, ensure handling conforms to legal requirements and determine the risks of collecting the information. Moreover, DOJ stated that the FBI's face recognition capabilities do not represent new collection, use, or sharing of personal information.

We acknowledge that DOJ agreed in part with our recommendation and submitted the SORN for publication after we provided our draft report for comment. However, we disagree with DOJ's interpretation regarding the legal requirements of a SORN. As previously explained in our report, the Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public through a SORN published in the Federal Register. According to OMB guidance, the purposes of the notice are to inform the public of the existence of systems of records; the kinds of information maintained; the kinds of individuals on whom information is maintained; the purposes for which they are used; and how individuals can exercise their rights under the Act. Further, DOJ's formal comments on our draft report acknowledge that the automated nature of face recognition technology and the sheer number of photos now available for searching raise important privacy and civil liberties considerations. We believe that the ability to perform automated searches of millions of photos is fundamentally different in nature and scope than manual review of individual photos, and the potential impact on privacy is equally fundamentally different. While DOJ published a SORN that addresses the collection and maintenance of photos accessed and used through the FBI's face recognition capabilities in May 2016, it did so more than four years after beginning to use NGI-IPS. As a result, we have revised our recommendation to reflect that DOJ should complete and publish SORNs prior to collecting and using information in new or revised systems of records. By assessing the SORN development process and

taking corrective actions to ensure timely development of future SORNs, the public would have a better understanding of how their personal information is being used and protected by DOJ components.

DOJ partially concurred with our recommendation that the FBI conduct audits to determine the extent to which users of NGI-IPS and biometric images specialists in FACE Services are conducting face image searches in accordance with CJIS policy requirements. Specifically:

- DOJ concurred with the portion of our recommendation related to the use of NGI-IPS. DOJ stated that the FBI did not specify policy requirements with which it could audit NGI-IPS users until late 2014, completed a draft audit plan during the course of our review in summer 2015, and expects to begin auditing use of NGI-IPS in fiscal year 2016.

- DOJ did not fully comment on the portion of the recommendation that the FBI audit the use of external databases.[61] As noted in the report, we understand the FBI may not have authority to audit the maintenance or operation of databases owned and managed by other agencies. However, the FBI does have a responsibility to oversee the use of the information by its own employees. As a result, our recommendation focuses on auditing both NGI-IPS users, such as states and FACE Services employees, as well as FACE Services employees' use of information received from external databases—not on auditing the external databases. We continue to believe that the FBI should audit biometric images specialists' use of information received from external databases to ensure compliance with FBI privacy policies.

DOJ did not concur with our recommendation that the FBI conduct tests of NGI-IPS to verify that the system is sufficiently accurate for all allowable candidate list sizes. In its response, DOJ stated that because searches of NGI-IPS produce a gallery of likely candidates to be used as investigative leads instead of for positive identification, NGI-IPS cannot produce false positives and there is no false positive rate for the system. DOJ further stated that the FBI has performed accuracy testing to validate

[61]In its formal comment letter, DOJ stated: "Though not entirely clear from the recommendation itself, it does not appear that GAO recommends that the FBI audit the use of external databases. DOJ would disagree with such a recommendation."

that the system meets the requirements for the detection rate, which fully satisfies requirements for the investigative lead service provided by NGI-IPS.

We disagree with DOJ. In its response, DOJ did not address a key focus of this recommendation—the need to ensure that NGI-IPS is sufficiently accurate for all allowable candidate list sizes. As stated in our report, although the FBI has tested the detection rate for a candidate list of 50 photos, NGI-IPS allows users to request smaller candidate lists—specifically between 2 and 50 photos. FBI officials stated that they have not tested the detection rate for smaller candidate list sizes and that a smaller candidate list would likely lower the detection rate. Further, as stated in our report, the National Science and Technology Council and the National Institute of Standards and Technology state that the detection rate and the false positive rate are both necessary to assess the accuracy of a face recognition system. Reporting a detection rate without reporting the accompanying false positive rate presents an incomplete view of the system's accuracy. We understand DOJ's position that the detection rate is the primary accuracy measure for NGI-IPS when returning a gallery of potential candidates and we have revised the wording of our recommendation to reflect that when the FBI tests the detection rate, it should identify both the detection rate and the false positive rate used to conduct the test. We continue to believe that our recommended action is needed and would allow the FBI to have more reasonable assurance that NGI-IPS is providing an investigative lead service that enhances, rather than hinders or overly burdens, criminal investigation work.

DOJ concurred with our recommendation that the FBI conduct an operational review of NGI-IPS that includes an assessment of the accuracy of face recognition searches. DOJ stated that the FBI plans to solicit user feedback through the Advisory Policy Board Process regarding whether the accuracy of NGI-IPS face recognition searches is meeting their needs. If fully implemented, this action should address the intent of the recommendation and affords the FBI more reasonable assurance that NGI-IPS is meeting federal, state, and local law enforcement needs.

DOJ did not concur our recommendation that the FBI take steps to determine whether external face recognition systems used by the FBI are sufficiently accurate for its use. DOJ stated that the FBI has no authority to set or enforce accuracy standards of face recognition technology operated by external agencies. In addition, DOJ stated that the FBI has

implemented standard operating procedures that include multiple layers of manual review that mitigate risks associated with the use of automated face recognition technology. Further, it is DOJ's position that there is value in searching all available external databases, regardless of their level of accuracy.

We disagree with DOJ. We continue to believe that the FBI should assess the quality of the data it is using from state and federal partners. We acknowledge that the FBI cannot and should not set accuracy standards for the face recognition systems used by external partners. We also do not dispute that the use of external face recognition systems by the FACE Services Unit could add value to FBI investigations. However, we disagree with FBI's assertion that no assessment of the quality of the data from state and federal partners is necessary. The FBI has entered into agreements with state and federal partners to conduct face recognition searches using over 380 million photos. Without actual assessments of the results from its state and federal partners, the FBI is making decisions to enter into agreements based on assumptions that the search results may provide valuable investigative leads. In addition, we disagree with DOJ's assertion that manual review of automated search results is sufficient. Even with a manual review process, the FBI could miss investigative leads if a partner does not have a sufficiently accurate system. Therefore, it is unclear whether such agreements are beneficial to the FBI and whether its investment of public resources is justified. By relying on its external partners' face recognition systems, the FBI is using these systems as a component of its routine operations and is therefore responsible for ensuring the systems will help meet FBI's mission, goals and objectives. We continue to believe that taking steps to determine whether external face recognition systems are sufficiently accurate would provide FBI with better assurance that the systems they use are appropriate for its use and would increase the odds of identifying suspects for active investigations while protecting privacy.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the Attorney General, and the Secretaries of the Departments of State and Defense. In addition, this report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-9627 or maurerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix V.

Sincerely yours,

Diana C. Maurer
Director, Homeland Security and Justice Issues

Appendix I: Objectives, Scope, and Methodology

This report addresses the following questions (1) What are the Federal Bureau of Investigation's (FBI) face recognition capabilities? (2) To what extent has FBI's use of face recognition adhered to laws and policies related to privacy? (3) To what extent does the FBI assess the accuracy of its face recognition capabilities? The scope of this report includes the FBI's use of face recognition technology for criminal investigations and focuses on the federal laws and policies by which FBI must abide.

To address the first question, we reviewed documentation of the mission need established to warrant FBI investment in face recognition technology, including the Next Generation Identification (NGI) Mission Needs Statement and the Face Analysis Comparison and Evaluation (FACE) Services Concept of Operations. In addition, we reviewed FBI documentation describing the FBI's face recognition technology capabilities, including the *NGI Interstate Photo System (NGI-IPS) Policy and Implementation Guide*,[1] the FACE Services Unit operating manual, and memorandums of understanding (MOUs) between the FBI and its federal and state partners. We reviewed these documents in order to understand the FBI's face recognition capabilities used for criminal investigations, the process for enrolling individuals into face recognition databases, the personnel authorized to conduct face recognition searches, and how the FBI and its partners conduct these searches. We also analyzed the MOUs between the FBI and states to determine the types of information states provide to FACE Services. Further, we visited the Criminal Justice Information Services (CJIS) facility in West Virginia to observe a demonstration of NGI-IPS. We reviewed the most recent FBI face recognition data available—August 2011 through December 2015 on the enrollment of individuals' photos in databases and the number of searches conducted on those databases to provide context to FBI's use of face recognition technology.

We also interviewed FBI officials responsible for face recognition technology used for criminal investigations to help us better understand face recognition capabilities within the FBI. To better understand how the FBI coordinates with federal and state partners and how these partners' face recognition databases are populated and maintained, we interviewed Department of State (State), Department of Defense (DOD), Michigan,

[1]See FBI Criminal Justice Information Services (CJIS) Division, *NGI-IPS Policy and Implementation Guide, version 1.2* (Clarksburg, WV: Sept. 3, 2014).

and Texas officials responsible for coordinating with the FBI's face recognition officials. We selected DOD and State because these are the only federal agencies with face recognition MOUs with the FBI. We selected Michigan and Texas because both states had agreements with the FBI that covered multiple face recognition capabilities.[2] We also received a demonstration of State's Consular Consolidated Database to better understand how FBI officials that access the database use it to conduct face recognition searches.

To address the second question, we identified and reviewed privacy protections under federal law, including the Privacy Act of 1974, the E-Government Act of 2002, and Office of Management and Budget guidance to determine DOJ and FBI statutory responsibilities related to protecting privacy of personal information in FBI's use of face recognition technology. We also reviewed DOJ privacy policies, including; *DOJ Order 0601: Privacy and Civil Liberties, the Senior Component Official on Privacy Manual*, and Privacy Impact Assessment (PIA) Guidance to better understand DOJ's privacy oversight structure and identify its PIA and system of records (SORN) development and review process.[3] In addition, we analyzed relevant public notices and disclosures published from 1999 through 2015, such as the FBI's published PIAs related to NGI and the SORN for the Fingerprint Identification Records System, to determine what the FBI has disclosed to the public regarding the personal information collected for its face recognition capabilities and how it uses the data. We also assessed the FBI's public notices and disclosures against legal and policy privacy requirements as well as the Fair Information Practice Principles.[4] Further, we analyzed documentation of

[2]Michigan, New Mexico, and Texas were the only states that had agreements with the FBI on NGI-IPS and FACE Services at the time of their selection. Selecting Michigan and Texas offered some geographic dispersion. While these selections are not generalizable to other states, we believe they provide important context into facial recognition capabilities at the state level.

[3]Department of Justice (DOJ), DOJ Order 0601: Privacy and Civil Liberties (Washington, D.C.: Feb. 2014); DOJ Office of Privacy and Civil Liberties, Senior Component Official on Privacy Manual, Spring 2014 (Washington, D.C.: June 2014); and DOJ Office of Privacy and Civil Liberties, Privacy Impact Assessments Official Guidance (Washington, D.C: Mar. 2012).

[4]For purposes of this review, we used the eight Fair Information Practice Principles developed by the U.S. Department of Homeland Security. These practices are transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, and accountability and auditing.

the FBI's mechanisms of oversight of its face recognition services with regards to privacy, such as audit reports and policies, and compared them to *Standards for Internal Control in the Federal Government* and the Fair Information Practice Principles to determine the extent to which the FBI oversees adherence to its privacy policies.[5]

We interviewed officials from DOJ's Office on Privacy and Civil Liberties (OPCL), the FBI's Privacy and Civil Liberties Unit, and CJIS to understand the general processes and procedures DOJ and the FBI have in place to ensure compliance with privacy statutory requirements related to FBI's use of face recognition technology and the extent to which the FBI has followed these processes and procedures. We also interviewed members of the FBI's Advisory Policy Board, and members of the Compact Council to understand their perspectives of statutory requirements, policies, and guiding principles related to the FBI's use of face recognition technology; processes for implementing statutory requirements; and the FBI's means for assessing privacy implications of the FBI's use of face recognition technology.[6] To identify the public's privacy concerns related to the FBI's use of face recognition technology, we interviewed privacy advocacy groups, including the Center for Democracy and Technology, the Electronic Privacy Information Center, and Electronic Frontier Foundation. We also interviewed relevant FBI officials and privacy stakeholders, including members from the Advisory Policy Board and Compact Council, to understand how the FBI coordinates with stakeholders, the privacy concerns stakeholders have discussed with the FBI, and how the FBI has addressed those concerns.

To address the third question, we reviewed FBI documents to identify the face recognition accuracy requirements the FBI established for NGI-IPS, including the NGI System Requirements Document and the NGI System Requirement Specification. We focused on the accuracy of the automated portion of the FBI's face recognition capabilities, though we took steps to understand the extent to which human review could affect accuracy as well. We reviewed system and contractual documents to understand how

[5]GAO, *Internal Control: Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: Nov. 1999).

[6]The Advisory Policy Board is responsible for reviewing appropriate policy, technical, and operational issues related to the FBI's CJIS Division. The Compact Council, on the other hand, is comprised of state and federal representatives and is responsible for setting policy regarding the sharing of criminal history records for non-criminal-justice purposes.

the accuracy requirements changed over the development of NGI-IPS. We reviewed NGI-IPS test results documented in the NGI Requirements Traceability Matrix and the System Acceptance Tests. We assessed the NGI-IPS test results against the testing requirements in the FBI's Information Technology Life Cycle Management Directive, and face recognition literature developed by the National Science and Technology Council and the National Institute of Standards and Technology. Further, we compared the FBI's efforts to conduct operational assessments on NGI-IPS to the FBI, DOJ, and Office of Management and Budget guidance—such as the FBI Information Technology Life Cycle Management Directive—and draft testing guidelines established by the Face Identification Scientific Working Group.[7] We also reviewed the National Institute of Standards and Technology's 2014 Face Recognition Vendor Test report to better understand the various face factors that impact the accuracy of face recognition systems and how it tested the accuracy of face recognition systems.[8] Further, we reviewed MOUs between the FBI and external partners—16 states, DOD, and State—to determine the extent to which the MOUs addressed accuracy of the face recognition technologies these partners use and the data they provide to the FBI. We compared the FBI's efforts to assess the accuracy of the face recognition systems operated by external partners to *Standards for Internal Controls in the Federal Government*.[9] Further, we assessed these efforts against the Fair Information Practice Principles. To learn more about how the FBI assesses NGI-IPS and the external systems it has access to for accuracy, we interviewed FBI officials, as well as officials from Michigan, Texas, DOD, and State. We also interviewed MorphoTrust, the company that provides the face recognition technology for NGI-IPS, and National Institute of Standards and Technology officials to better understand the accuracy of face recognition systems in general.

[7]See FBI, *FBI Information Technology Life Cycle Management Directive*, version 3.0 (August 19, 2005), DOJ, *Systems Development Life Cycle Guidance* (January 2003), OMB, *Circular No. A-11, Planning, Budgeting, and Acquisition of Capital Assets*, V 3.0 (2015), and Face Identification Scientific Working Group, *Understanding and Testing for Face Recognition Systems Operation Assurance, version* 1.0 (Aug. 15, 2014).

[8]National Institute of Standards and Technology, *Face Recognition Vendor Test: NIST Interagency Report 8009* (May 26, 2014).

[9]GAO/AIMD-00-21.3.1.

We conducted this performance audit from January 2015 to May 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: FBI Face Recognition Summary Statistics

Next Generation Identification (NGI) History and Summary Statistics

The NGI system is a replacement for the FBI's Integrated Automated Fingerprint Identification System (IAFIS), which was a national, computerized system for storing, comparing, and exchanging fingerprint data in a digital format. NGI was not only to include fingerprint data from IAFIS, but also to provide new functionality and improve existing capabilities by incorporating advancements in biometrics, such as face recognition. As part of the fourth of six increments, the FBI updated the Interstate Photo System (IPS) to provide a face recognition service that allows law enforcement agencies to search a database of criminal photos that accompanied a fingerprint submission using a probe photo.[1] The FBI began a pilot of NGI-IPS in December 2011, and NGI-IPS became fully operational in April 2015. Over 80 percent of the photos in NGI-IPS are criminal, as shown in table 3 below.

Table 3: Number of Searchable Criminal Photos and Civil Photos Enrolled by State and Federal Agencies in Next Generation Identification-Interstate Photo System (NGI-IPS), as of December 2015

Submitting Entity	Searchable Criminal Photos (millions)	Civil Photos (millions)
States and territories	19.4	0.9
Federal agencies	5.5	3.9
Total	**24.9**	**4.8**

Source: GAO analysis of FBI data. |GAO-16-267

- Texas and Louisiana are the states with the largest number of criminal photo contributions, with over three million submissions for each state. Other states with large criminal photo submissions are: Michigan (2.3 million), Virginia (1.8 million), California (1.7 million), and New York (1.4 million). U.S. Customs and Border Protection is the largest federal contributor of criminal photos, with approximately 2.4 million submissions, which accounts for almost half of the total federal criminal photos. Over 2.5 million photos have been rejected from submitting entities due to poor quality as of December 2015.

[1]When the FBI implemented IAFIS in 1999, the Criminal Justice Information Services (CJIS) Division began storing mugshots submitted with fingerprints in a photo database and also digitized all previously submitted hardcopy mugshots. However, until NGI, this database did not allow users to search for mugshots using information other than the person's name or unique FBI number

- Local, state, federal, and tribal law enforcement agencies can be authorized to submit face recognition searches for law enforcement purposes.[2] From the beginning of the pilot in December 2011 through December 2015, the number of search requests by states ranged from under 20 by one state to over 14,000 by another state.

Facial Analysis, Comparison, and Evaluation (FACE) Services Summary Statistics

FACE Services—a unit within the FBI's Criminal Justice Information Services Division (CJIS)—conducts searches on NGI-IPS and can access external partners' face recognition systems to support FBI active investigations only.[3] Table 4 shows the number of searchable photos accessible to FACE Services through all available databases.

Table 4: Number of Photos Available to Facial Analysis, Comparison, and Evaluation (FACE) Services by Repository as of December 2015

Searchable Repository	Description of photos in the repository	Number of photos[a] (millions)
Federal Repositories		
Department of Defense's Automated Biometric Identification System	Individuals detained by U.S. forces abroad, among others	6.7
Next Generation Identification - Interstate Photo System (NGI-IPS)	Criminal and civil mug shots[b]	29.7
Department of State's Consular Consolidated Database	Visa application[c]	140
State Repositories		
North Dakota	Driver's license, criminal mugshots, correction photos	1.2
Vermont	Driver's license	1.8
New Mexico	Driver's license	2.9

[2]Authorized law enforcement users are those with an Originating Agency Identifier designating the user as a law enforcement agency including a unit or subunit of a local, state, federal or tribal government with the principle functions of prevention, detection, and investigation of crime, apprehension of alleged offenders, and enforcement of laws.

[3]According to the *Privacy Impact Assessment for the FACE Services Unit*, in limited instances, the FACE Services Unit provides face recognition support for closed FBI cases (e.g., missing and wanted persons) and may offer face recognition support to federal partners.

Searchable Repository	Description of photos in the repository	Number of photos[a] (millions)
Delaware	Driver's license	4
Utah	Driver's license, criminal mugshots, correction photos	5.2
Alabama	Driver's license	6.5
Nebraska	Driver's license	8
South Carolina	Driver's license, criminal mugshots, probation photos	8
Tennessee	Driver's license	12.5
Iowa	Driver's license	13
Arkansas	Driver's license	15.4
Kentucky	Driver's license	18.4
Texas	Driver's license	24
Michigan	Driver's license, criminal mugshots, correction photos	35.6
North Carolina	Driver's license	36
Illinois	Driver's license	43
Total		**411.9**

Source: GAO analysis FBI information.|GAO-16-267

[a]According to the FBI, the numbers for the repositories other than NGI-IPS were confirmed at the time the MOU with the partner agency was signed.

[b]The face recognition search is only conducted on NGI-IPS's criminal database. However, civil photos may be returned in the search of the criminal database if they are linked to a criminal identity record.

[c]In October 2015, State and the FBI initiated a 180 day pilot for State to conduct face recognition comparisons of persons under FBI investigation against passport photos in the State passport database.

FACE Services can either access directly or request searches from partners' databases. From August 2011 through December 2015, FACE Services received over 142,000 photos of unknown persons (often called probe photos) from FBI headquarters, field offices, and overseas offices, which resulted in almost 215,000 searches on various databases in attempt to find photo matches of known individuals in these databases. Table 5 summarizes the number of searches requested or conducted by FACE Services and the number of photos returned to requesting FBI agents, from August 2011 through December 2015.

Table 5: Summary of Facial Analysis, Comparison, and Evaluation (FACE) Services Unit Searches and Photos Retuned to Agents from August 2011 through December 2015

	Approximate number of face recognition searches requested or conducted by FACE Services	Approximate number of searches resulting in likely candidates that FACE Services returned to requesting FBI agents
Next Generation Identification -Interstate Photo System (NGI-IPS)	118,490[a]	6,050
Department of Defense's Automated Biometric Identification System	8,220[b]	60
Department of State's Consular Consolidated Database	51,720	2,270
Department of State's Passport Photos	70	Less than 10
16 states	36,420[c]	210
Total	**214,920**	**8,590**

Source: GAO analysis of FBI data.| GAO-16-267

[a]Although over 142,000 probe photos were received by FACE Services, multiple photos of the same individual may have been received and not necessarily searched by biometric images specialists.

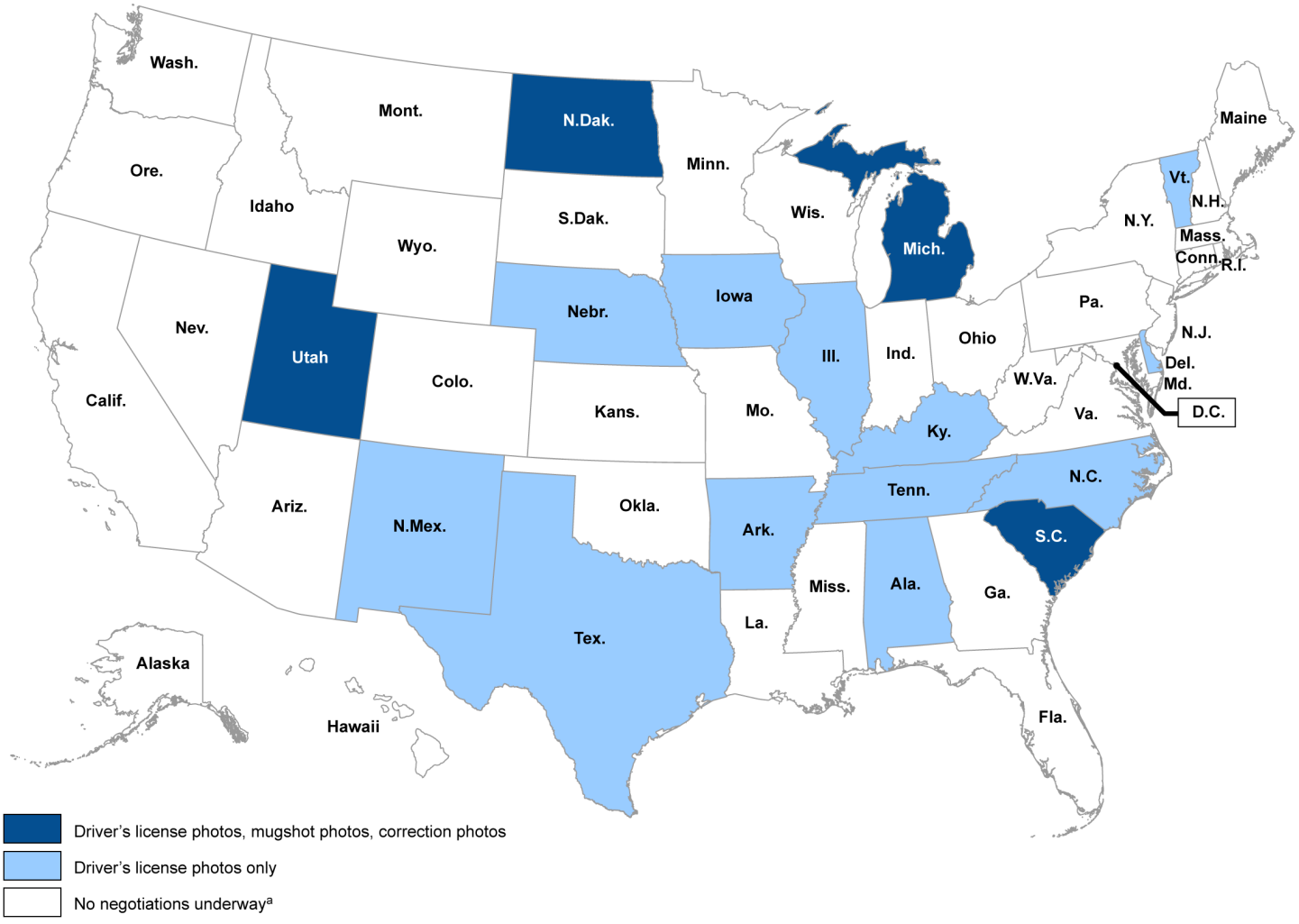
[b]The Department of Defense does not return face images, unless the FBI follows-up with a request based on the Automated Biometric Identification System search results.

[c]This is the combined total of searches submitted to all 16 participating states.

Appendix III: States Partnered with FBI's Facial Analysis, Comparison, and Evaluation (FACE) Services Unit

FACE Services—a unit within the FBI's Criminal Justice Information Services Division (CJIS)—conducts face recognition searches on Next Generation Identification-Interstate Photo System (NGI-IPS) and can access external partners' face recognition systems to support FBI active investigations. Figure 4 shows that, as of December 2015, FBI has signed Memorandums of Understanding (MOU) with 16 states to be able to request face recognition searches of the states' photo repositories to assist with FACE Services requests. Most of these systems access driver's license photos, but several states also include mugshots or corrections photos.

Figure 4: Information Available for FBI Facial Analysis, Comparison, and Evaluation (FACE) Services' Photo Searches, by State



Source: GAO analysis of FBI information; Map Resources (map). | GAO-16-267

[a]Some state laws prohibit face recognition.

Appendix IV: Comments from the Department of Justice

U.S. Department of Justice

Washington, D.C. 20530

APR 25 2016

Diana Maurer
Director, Homeland Security and Justice Issues
Government Accountability Office (GAO)
441 G Street N.W.
Washington, DC 20548

Dear Ms. Maurer:

Thank you for the opportunity to review and comment on your draft report titled "*GAO's Review of FBI's Use of Facial Recognition Technology* (GAO-15-11/441270). In this report, the Government Accountability Office ("GAO") made four recommendations based on their findings. This letter represents the consolidated Department ("DOJ" or "Department") response to GAO's recommendations.

I. Introduction

The Department (DOJ) disagrees with one of the two recommendations addressed to the Attorney General and agrees with the other. Further, the DOJ concurs with Recommendations 1 and 3 made to the Director of the FBI, partially agrees with recommendation 2 and disagrees with Recommendation 4.

The Federal Bureau of Investigation ("FBI") welcomed GAO to visit its Criminal Justice Information Services ("CJIS") Division to learn about its facial recognition processes. During GAO's visit[1], FBI CJIS' biometric images specialists provided a face recognition demonstration, and staff provided various briefings. During the year-long audit process, the FBI and the Office of Privacy and Civil Liberties (OPCL)[2] also responded to more than 20 document requests from GAO as well as participated in several teleconferences and in-person meetings to answer questions from GAO. Despite the voluminous amount of hours spent by FBI staff providing face recognition information to GAO, the FBI believes GAO staff does not fully appreciate the nature of its face recognition service as being utilized for investigative leads only and not positive identifications. Standards for accuracy can be reasonably different for systems that provide investigative leads as opposed to systems that provide positive identification, thus explaining the

[1] This visit occurred on April 14-15, 2015 at CJIS facilities in West Virginia.
[2] Please note the correct name of OPCL stands for Office of Privacy and Civil Liberties. Throughout the report, OPCL is incorrectly referred to as the Office on Privacy and Civil Liberties.

DOJ's disagreement with some of GAO's recommendations. In addition, the Department fundamentally disagrees with GAO's understanding of the purpose of a System of Records Notice (SORN).[3]

II. GAO's Recommendations and DOJ's Responses

Recommendation Number 1 to the Attorney General: Assess the PIA development process to determine why PIAs were not published prior to using or updating face recognition capabilities, and implement corrective actions to ensure the timely development, updating, and publishing of PIAs before using or making changes to a system.

- DOJ Response: Disagree, with explanation. While we agree that all Department processes may be reviewed for improvements and efficiencies, DOJ disagrees with the PIA rationale articulated in GAO's report for the reasons set forth below. Furthermore, DOJ continually strives to assess and refine its internal processes and procedures. As part of that ongoing review, DOJ will internally evaluate and improve upon the PIA process independent of this GAO review.

Privacy Impact Assessments (PIAs) for the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit and the Next Generation Identification (NGI) Interstate Photo System (IPS) have been prepared by the FBI, approved by the Chief Privacy and Civil Liberties Officer at the Department, and are published at https://www.fbi.gov/foia/privacy-impact-assessments. These PIAs provide the public with an accurate and complete explanation of how specific FBI components are using face recognition technology in support of the FBI's mission to defend against terrorism and enforce criminal laws, while protecting privacy and civil liberties. The PIAs also reflect many of the privacy and civil liberties choices made during the implementation of these programs.

Pursuant to DOJ policy, a Privacy Threshold Analysis (PTA) was prepared for FBI's Face Services Unit, as well as other significant documentation protecting privacy and civil liberties, such as Memoranda of Understanding and policy documentation – all of which built in privacy and civil liberties protections.

The FACE Services Unit provides face recognition support for FBI agents and analysts, and this internal support required no new collection, use, or sharing of personal data. As a new FBI unit, the FACE Services Unit proceeded carefully and deliberately. As such, the privacy documentation and guidance have been in development since the inception of the unit, incrementally changing and adding protections as decisions were made regarding the services provided. In addition, the work of the FACE Services Unit utilized information already covered by an existing system of records notice (SORN). The work log used by the FACE Services Unit retains only those photos already retained in the FBI's investigative case file system. The FACE

[3] A System of Records Notice (SORN) is a legal notice document required by the Privacy Act of 1974 which describes the existence and character of a system of records, including the categories of individuals whose records are in the system; the categories of records; and the routine uses of the records.

Services Unit's work log and the FBI's investigative files are currently covered by the FBI's Central Records System SORN (https://www.gpo.gov/fdsys/pkg/FR-1998-02-20/pdf/98-4206.pdf, 8671).

For the NGI-IPS system, the FBI published a PIA in 2008 that addressed the planned photo repository in NGI that would offer face recognition searching as one of its services. NGI had been implemented in increments over a period of several years, with major enhancements such as searching and retention of civil fingerprints, improved searching of latent fingerprints, and the development of a palm print repository. The relevant PIAs were prepared in tandem with these increments; the NGI-IPS became operational in the spring of 2015, as the last significant enhancement of NGI.

New privacy documentation and guidance were developed for the IPS starting in 2011. At that time, the FBI launched a "pilot" phase of face recognition technology with a few law enforcement partners in order to validate technical and user requirements. This pilot was conducted with mugshots already retained by the FBI in NGI's predecessor system, the Integrated Automated Fingerprint Identification System (IAFIS) (covered by the Fingerprint Identification Records System SORN, https://www.gpo.gov/fdsys/pkg/FR-1999-09-28/pdf/99-24989.pdf, 52347). In the interim between the pilot phase and full operational capability in 2015, the FBI prepared a PTA and other significant documentation, such as Memoranda of Understanding and a detailed Policy and Implementation Guide for future users of the face recognition service, memorializing the privacy and civil liberties protections being implemented. The FBI completed the 2015 NGI-IPS PIA prior to operational deployment.

The NGI-IPS and the FACE Services Unit PIAs, not the NGI SORN, represent the best resource for the public to learn about how face recognition technology is used. The NGI SORN covers the largest information technology system ever developed by the FBI and a SORN is not intended to provide the same level of detail to the public as a PIA. In order to provide the most transparency for the public and most detail on specific aspects of NGI, the FBI wrote several PIAs to cover the entire system in a meaningful and accurate manner. The primary purpose of NGI is to serve as the nation's premier fingerprint repository (criminal, civil, and latent) and the nation's central repository for the exchange of criminal history record information. The FBI had been writing the NGI-specific SORN as the system has been developed. The NGI SORN now specifically includes "facial images" as information associated with criminal history records; however, the NGI SORN covers the same category of individuals and photos associated with criminal history (*e.g.* "mugshots") that have been collected and retained by the FBI for decades, as reflected in the IAFIS SORN. Accordingly, the NGI-IPS PIA provides the most robust explanation of how face recognition technology is used to search records related to individuals who were already maintained by the FBI.

The FBI's existing legal authorities and data holdings were the basis for the authorized use of face recognition technology in its FACE Services Unit and its NGI-IPS. Prior to this technology, the photos used in the face recognition searches were retained or available to the FBI for human review in accordance with all laws and policies. For face recognition technology, the categories

of photos permitted to be searched have been carefully defined and limited in order to protect privacy and civil liberties.

For the FACE Services Unit, only those photos provided by FBI agents, legally obtained in the course of FBI investigations, may be accepted for searching. The levels and types of investigations for which searches are allowed have been limited to protect privacy and civil liberties. The FBI opens investigations pursuant to Attorney General Guidelines and implementing policy. These photos, as with any other investigative lead or evidence, cannot be collected in violation of an individual's constitutional rights.

In strict compliance with state and federal law, the FACE Services Unit searches the FBI photos against photo repositories maintained by other government agencies. These photo repositories specifically permit searching for law enforcement purposes and would be available to FBI agents regardless of face recognition technology. When photos are returned from these repositories, a trained biometric images specialist and a supervisor/lead employee in the FACE Services Unit provide reviews before forwarding to the FBI agent. The FBI agent is permitted to use the photo only as an investigative lead and must perform additional analysis to determine true identification. In the past, an FBI agent could manually review any available photo in the search for a subject. With face recognition technology, there is a three-part process: the software narrows the possible candidates, the trained biometric images specialist and supervisor/lead employee provide human reviews, and the agent decides whether to pursue a lead and investigate further.

For the NGI-IPS, only criminal mugshots obtained pursuant to arrest and associated with ten-print fingerprints are available for face recognition searching by law enforcement officers in accordance with the existing IAFIS SORN. Criminal photos that do not meet a probable cause standard or that are not positively associated with criminal fingerprints are not available for searching. The FBI also has the legal authority to retain civil photos in NGI when collected in conjunction with non-criminal justice fingerprint-based background checks. However, in order to protect privacy and civil liberties, the FBI decided not to permit searching of civil photos even though they may be helpful to law enforcement.

Access to NGI is generally available to the criminal justice community, who, by federal regulation, consists of a broader group of users than law enforcement. The FBI chose to limit face recognition searches to sworn law enforcement officers to ensure that such searches only pertained to active investigations and those searches were not used for purposes contrary to the IAFIS SORN. Law enforcement partners may submit investigative photos to search against the NGI-IPS mugshots. These photos are prohibited from being obtained in violation of constitutional rights. Importantly, these photos merely search against the NGI-IPS and are not retained. If the law enforcement officer receives photos from the NGI-IPS in response, he or she is advised that the photos are investigative leads and may not serve as the sole basis for independent law enforcement action.

As parts of a federal executive agency, DOJ and FBI comply with the Privacy Act of 1974.[4] The FBI observes that the Fair Information Practice Principles (FIPPs) predate the Privacy Act of 1974 and many of the Privacy Act requirements are similar to FIPPs guidance, such as transparency, notice, consent, and redress. However, the Privacy Act of 1974 permits federal agencies to exempt their law enforcement systems from these requirements due to the nature of information obtained from criminal subjects or in the course of criminal investigations. Since the photos maintained and searched in the FBI's Central Records System and NGI are law enforcement subjects, the FBI has exercised its exemptions under the Privacy Act. In its implementation of face recognition technology, the FBI has followed the FIPPs guidance to the fullest extent practicable in areas such as data minimization, use limitation, and data quality and integrity.

The FBI fully recognizes that the automated nature of face recognition technology and the sheer number of photos now available for searching raise important privacy and civil liberties considerations. For that reason, the FBI has made privacy and civil liberties integral to every decision from the inception regarding its use of face recognition technology. Documenting those decisions in the PIAs and other privacy and policy documentation, the FBI has established practices that protect privacy and civil liberties beyond the requirements of the law. Although the GAO report states that the FBI should better ensure privacy, it is important to note that the FBI observes that the GAO made no findings or recommendations regarding the sufficiency of the documented protections for face recognition technology implemented by the FACE Services Unit and in the NGI-IPS. The FBI has successfully used face recognition technology to further its mission to protect the American public from harm, while carefully and deliberately building privacy and civil liberties protections into the technology and providing the public with transparency through the published PIAs.

Recommendation Number 2 to Attorney General: Complete a SORN for the NGI system that addresses the collection and maintenance of photos accessed and used through the FBI's face recognition capabilities.

- DOJ Response: Agree in part. The SORN has been completed and submitted for publication to the Federal Register on April 21, 2016.[5]

Although the SORN has been submitted for publication to the Federal Register, the Department disagrees with GAO's conflation of the SORN requirement with the purpose of a PIA. SORNs are primarily used as a legal notice document under the Privacy Act.[6] In contrast, a PIA is an analysis, required by Section 208 of the E-Government Act of 2002, of how information in identifiable form is processed to: ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; determine the risks and effects of collecting, maintaining,

[4] *See* 5 U.S.C. § 552a (2012).

[5] The preparation of the NGI SORN predated the GAO audit to accommodate the various increments of the NGI program.

[6] *See* 5 U.S.C. § 552a (e) (4) (2012).

and disseminating information in identifiable form in an electronic information system; and examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[7]

To the extent that this GAO report may impact the privacy compliance of other Department components, OPCL notes the legal distinctions between a SORN and a PIA. Stated another way, a PIA is not a SORN. The determination to draft a SORN or provide a modification to an existing SORN is based on the legal requirements of the Privacy Act and Office of Management and Budget (OMB) guidance. This iterative process requires that a SORN may need to be reviewed for legal sufficiency to ensure its continuing completeness and accuracy, but may not necessarily need to be updated.

Recommendation Number 1 to FBI Director: To better ensure that face recognition capabilities are being used in accordance with privacy protection laws and policy requirements, we recommend that the Director of the Federal Bureau of Investigation conduct audits to determine the extent to which users of NGI-IPS and biometric images specialists in the FACE Services Unit are conducting face image searches in accordance with CJIS policy requirements.

- The DOJ concurs with this recommendation to the extent it relates to use of the NGI-IPS.[8]

GAO's findings reflect that state and local users have been accessing the NGI-IPS since December 2011, and users have yet to be audited for their use of face recognition searches. The DOJ agrees with and certainly appreciates GAO's assertion that audits serve an important role in identifying and mitigating risks associated with users of information systems not meeting policy requirements. However, as described on pages 11 and 12 of the report, it is important to recognize the NGI-IPS operated in a limited capacity as a pilot program from December 2011 through April 2015. The FBI Criminal Justice Information Services (CJIS) Division's Audit Unit (CAU) has no direct mandate to audit pilot phases of CJIS system development and implementation, and the CAU's triennial audit obligations pursuant to the *CJIS Security Policy* have not been historically interpreted to mandate such reviews.

In addition, the CAU does not complete development and implementation of formal audit processes until specific policy requirements for the CJIS system have been identified and finalized. This appears to be consistent with published *GAO Government Auditing Standards* for identifying audit criteria and associated considerations for obtaining sufficient, appropriate evidence as it relates to field work standards for performance audits. These standards include identification of "specific requirements, measures, expected performance, defined business

[7] OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Attachment A, Section II.A.6 (Sept. 26, 2003), *available at*: http://www.whitehouse.gov/omb/memoranda_M-03-22.

[8] Though not entirely clear from the recommendation itself, it does not appear that GAO recommends that the FBI audit the use of external databases. DOJ would disagree with such a recommendation.

practices, and benchmarks against which performance is compared or evaluated." Specific policy requirements associated with access to the NGI-IPS were not formally established until late 2014 with the approval and publishing of the *NGI-IPS Policy and Implementation Guide*, which was a primary resource for development of the audit objective, scope, and methodology. While the early stages of planning for formal NGI-IPS audits began during the system's pilot phase and prior to GAO's review, the formal draft audit plan was completed on schedule in summer 2015 and immediately submitted through the CJIS Advisory Policy Board (APB) process for review.

The CJIS APB Working Groups reviewed the plan in March 2016, and the audit plan will be reviewed by applicable subcommittees and the full CJIS APB at respective meetings in April and June 2016. As a result, an officially approved audit plan could not be provided to GAO. The DOJ did, however, make CAU officials available to GAO throughout the review process and all questions regarding plans to audit NGI-IPS were answered.

As planned, the CAU is fully postured to launch the first phase of the NGI-IPS audit plan as part of the existing fiscal year 2016 audit schedule, although the number of actual NGI-IPS participants is currently limited. The NGI-IPS audit will be conducted in conjunction with existing National Identity Services Audits externally at State Identification Bureaus and federal agencies and will include reviews at a selection of local criminal justice agencies that access the NGI-IPS. The NGI-IPS audit plan also provides for an internal audit of the FACE Services Unit to be conducted in accordance with existing procedures for FBI internal audits associated with CJIS system access. Procedures for both external and internal audits include review of NGI-IPS system transaction records and associated supporting documentation provided by audit participants.

GAO's last three recommendations focus on accuracy. The FBI would like to clarify terminology used by GAO in relation to the accuracy of face recognition technology. The FBI defines accuracy as the facial recognition technology's ability to return a photo representing one person's face in the search result (*e.g.*, candidate list of a fixed size) when a corresponding photo of that same person is enrolled in the face repository being searched. When referring to "detection" for face recognition purposes, this usually means the simple ability of a face recognition system to detect the presence of a face in a given image. Detection is a prerequisite for recognition – if a face is not detected, recognition cannot take place. In GAO's report, "detection" and the detection rate refer to the likelihood of a face recognition system to return a photo in the search result when the person's photo is in the repository of photos being searched.

The use of identification and recognition in the context of the FBI's performance of face recognition does not imply the determination of a "likely candidate" is the same person to the exclusion of all others. Positive identification would only occur with a face recognition system that has the capability to verify a match of the probe photo image to a photo image in the repository of photos being searched. The FBI is unaware of any facial recognition technology with sufficient accuracy to produce positive identifications; they instead produce likely candidates in the results. A false positive identification would occur when a system has the capability to produce a positive identification for one person, yet returns as the search result a

photo of a different person. In the absence of facial recognition systems with the capability to produce positive identifications, there are also no false positive identifications. Because the FBI does not use a system which generates positive identifications, there are no false positive identifications generated, so there is no false positive rate.

Recommendation Number 2 to FBI Director: Conduct tests of NGI-IPS to verify that the system is sufficiently accurate for all allowable candidate sizes, including setting and testing detection and false positive rates.

- **Response**: The DOJ disagrees with this recommendation. As FBI staff advised GAO, a search of the NGI-IPS provides a gallery of likely candidates that are to be used as investigative leads. A search of the NGI-IPS does not result in a positive identification; there are no identity matches based on a probe photo being searched against the photos in the NGI-IPS. As stated earlier, due to the fact that no positive identifications are made based on NGI-IPS searches, there are also no false positive identifications. As noted in the report, the FBI has performed accuracy testing to validate that the system meets the requirements for the detection rate, and such testing continues to be included as part of the FBI's standard testing and regression efforts. This fully satisfies requirements for the investigative lead service provided by the NGI-IPS and was confirmed by the Chief of the National Institute of Standards and Technology's Information Access Division.

Recommendation Number 3 to FBI Director: Conduct an operational review of NGI-IPS at least annually that includes an assessment of the accuracy of face recognition searches to determine if it is meeting federal, state, and local law enforcement needs and take actions, as necessary, to improve the system.

- **Response**: The DOJ concurs with this recommendation.

The FBI manages the CJIS APB Process, which holds meetings twice a year. The APB is comprised of members of local, state, tribal, and federal criminal justice agencies that contribute to and use CJIS systems and information. It is responsible for reviewing policy issues and appropriate technical and operational issues related to FBI CJIS programs (such as the NGI) administered by the FBI's CJIS Division, and thereafter, making appropriate recommendations. Through the APB Process, users can provide feedback and suggestions or bring issues to the attention of the FBI's CJIS Division.

To date, no users have submitted concerns to the FBI regarding the accuracy of face searches conducted on the NGI-IPS. However, in a proactive effort to conduct an operational review of the NGI-IPS to include an assessment of the accuracy of face recognition searches, the FBI plans to solicit user feedback through the APB Process regarding whether the face recognition searches

of the NGI-IPS are meeting their needs, specifically requesting input regarding search accuracy. Based on feedback, the FBI will take action, as necessary, to improve the system. The FBI can continue to solicit feedback through the APB Process on an as-needed basis.

Recommendation Number 4 to FBI Director: Take steps to determine whether each external face recognition system used by the FACE Services Unit is sufficiently accurate for the FBI's use and whether results from those systems should continue to be used to support FBI investigations.

- **Response**: The DOJ disagrees with this recommendation.

The FBI has no authority to set or enforce accuracy standards of face recognition technology operated by external agencies. Also, when considering the accuracy of external face recognition systems, it is important to understand that when searches are conducted in these systems, results returned to the FBI are only used as investigative leads. They are not considered to be positive identification. Furthermore, the FBI reduces any potential risks of searching external face recognition systems by several levels of manual review, to include reviews by trained experts. Two biometric images specialists are required to perform independent analysis, comparisons, and evaluations of all candidates (investigative leads) returned from face recognition searches. Then a supervisor/lead employee is required to review the results to determine if they may provide any value as investigative leads prior to routing them to FBI agents for their consideration in investigations. Lastly, the FBI agents make the final determination on the value of these responses relative to the investigation. These multiple levels of manual review minimize the risks associated with using automated systems for face recognition.

The FBI understands that the searches of external face recognition systems may not result in a response (investigative lead), as is the case with any search conducted in criminal justice information systems, but it doesn't negate the value of conducting the searches. Increasing the number of facial recognition systems that are leveraged for the FBI's face recognition searches increases the likelihood of obtaining valuable investigative leads. Conversely, for the FBI to not take advantage of the opportunity to search external facial recognition systems would be to give up opportunities to provide valuable investigative leads in support of criminal, terrorism, and missing person investigations.

Therefore, based on the increased reliability on the accuracy of face recognition systems over the past few years, the FBI's manual reviews by experts of all investigative leads provided as search results, and the value added to FBI investigations from the searches that have been conducted, the FBI is confident in its decision to continue searching external face recognition systems to support FBI investigations.

III. Conclusion

Thank you again for the opportunity to review and comment on this report. We look forward to GAO closing those recommendations that the DOJ has agreed to implement.

Sincerely,

Lee J. Lofthus
Assistant Attorney General
for Administration

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Diana C. Maurer, at (202) 512-9627 or maurerd@gao.gov

Staff Acknowledgments

In addition to the contact named above, Dawn Locke (Assistant Director) and Paul Hobart (Analyst-in-Charge) managed the work. Also, Jennifer Beddor, Orlando Copeland, Chris Currie, Michele Fejfar, John de Ferrari, Eric Hauswirth, Susan Hsu, Richard Hung, Monica Kelly, Susanna Kuebler, Alexis Olson, David Plocher, and Janet Temko-Blinder, made key contributions to this report.