United States Government Accountability Office

Testimony

Before the Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 9:30 a.m. ET
Wednesday, March 22, 2017

FACE RECOGNITION TECHNOLOGY

DOJ and FBI Need to Take Additional Actions to Ensure Privacy and Accuracy

Statement of Diana Maurer, Director,
Homeland Security and Justice

Accessible Version

GAO-17-489T

March 2017

FACE RECOGNITION TECHNOLOGY

DOJ and FBI Need to Take Additional Actions to Ensure Privacy and Accuracy

GAO Highlights

Highlights of GAO-17-489T, a testimony before the Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

Technology advancements have increased the overall accuracy of automated face recognition over the past few decades. This technology has helped law enforcement agencies identify criminals in their investigations. However, privacy advocates and members of the Congress remain concerned regarding the accuracy of the technology and the protection of privacy and individual civil liberties when technologies are used to identify people based on their biological and behavioral characteristics.

This statement describes the extent to which the FBI ensures adherence to laws and policies related to privacy regarding its use of face recognition technology, and ensure its face recognition capabilities are sufficiently accurate. This statement is based on our May 2016 report regarding the FBI's use of face recognition technology and includes agency updates to our recommendations. To conduct that work, GAO reviewed federal privacy laws, FBI policies, operating manuals, and other documentation on its face recognition capability. GAO interviewed officials from the FBI and the Departments of Defense and State, which coordinate with the FBI on face recognition. GAO also interviewed two state agencies that partner with FBI to use multiple face recognition capabilities.

What GAO Recommends

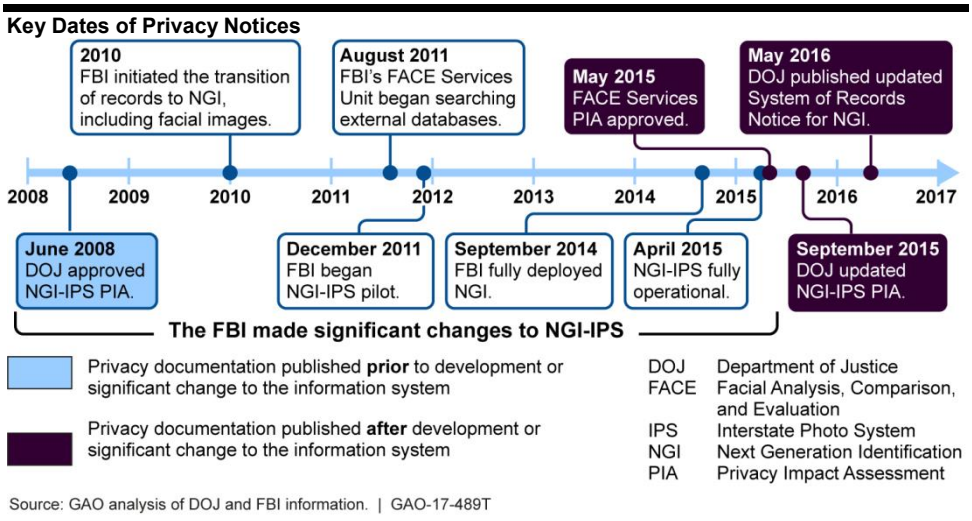
In May 2016, DOJ and the FBI partially agreed with two recommendations and disagreed with another on privacy. FBI agreed with one and disagreed with two recommendations on accuracy. GAO continues to believe that the recommendations are valid.

View GAO-17-489T. For more information, contact Diana Maurer at (202) 512-8777or maurerd@gao.gov.

What GAO Found

In May 2016, GAO found that the Federal Bureau of Investigation (FBI) had not fully adhered to privacy laws and policies and had not taken sufficient action to help ensure accuracy of its face recognition technology. GAO made six recommendations to address these issues. As of March 2017, the Department of Justice (DOJ) and the FBI disagreed with three recommendations and had taken some actions to address the remainder, but had not fully implemented them.

Privacy notices not timely. In May 2016, GAO recommended DOJ determine why privacy impact assessments (PIA) were not published in a timely manner (as required by law) and take corrective action. GAO made this recommendation because FBI did not update the Next Generation Identification-Interstate Photo System (NGI-IPS) PIA in a timely manner when the system underwent significant changes or publish a PIA for Facial Analysis, Comparison and Evaluation (FACE) Services before that unit began supporting FBI agents. DOJ disagreed on assessing the PIA process stating it established practices that protect privacy and civil liberties beyond the requirements of the law. GAO also recommended DOJ publish a system of records notice (SORN) and assess that process. DOJ agreed to publish a SORN, but did not agree there was a legal requirement to do so. GAO believes both recommendations are valid to keep the public informed on how personal information is being used and protected by DOJ components.



Source: GAO analysis of DOJ and FBI information. | GAO-17-489T

GAO also recommended the FBI conduct audits to determine if users of NGI-IPS and biometric images specialists in the FBI's FACE Services unit are conducting face image searches in accordance with DOJ policy requirements. The FBI began conducting NGI-IPS user audits in 2017.

Accuracy testing limited. In May 2016, GAO recommended the FBI conduct tests to verify that NGI-IPS is accurate for all allowable candidate list sizes to give more reasonable assurance that NGI-IPS provides leads that help enhance criminal investigations. GAO made this recommendation because 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. GAO also recommended the FBI take steps to determine whether systems used by external partners are sufficiently accurate for FBI's use. By taking such steps, the FBI could better ensure the data from external partners do not unnecessarily include photos of innocent people as investigative leads. However, FBI disagreed with these two recommendations, stating the testing results satisfy requirements for providing investigative leads and that FBI does not have authority to set accuracy requirements for external systems. GAO continues to believe these recommendations are valid because the recommended testing and determination of accuracy of external systems would give the FBI more reasonable assurance that the systems provide investigative leads that help enhance, rather than hinder or overly burden, criminal investigation work.

GAO also recommended the FBI conduct an annual operational review of NGI-IPS to determine if the accuracy of face recognition searches is meeting federal, state, and local law enforcement needs and take actions, as necessary. DOJ agreed and in 2017 FBI stated they implemented the recommendation by submitting a paper to solicit feedback from NGI-IPS users on whether face recognition searches are meeting their needs. However, GAO believes these actions do not fully meet the recommendation because they did not result in any formal response from users and did not constitute an operational review. GAO continues to recommend FBI conduct an operational review of NGI-IPS at least annually.

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee:

I am pleased to be here today to discuss our work on the Federal Bureau of Investigation's (FBI) use of face recognition technology. As the law enforcement community adopts face recognition technology for investigative purposes, academics, privacy advocates, and members of the Congress have questioned whether it is sufficiently accurate for this use. In addition, the use of face recognition technology raises questions regarding the protection of privacy and individual civil liberties. Face recognition technology mimics how people identify others: by scrutinizing their face. However, what is an effortless skill in humans has proven difficult to replicate in machines, although computer and technology advancements over the past few decades have increased the overall accuracy of automated face recognition. According to officials from the 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.

This statement describes the extent to which the FBI (1) ensures adherence to laws and policies related to privacy regarding its use of face recognition technology, and (2) ensures its face recognition capabilities are sufficiently accurate. This statement is based on our prior work issued in May 2016 regarding the FBI's use of face recognition technology and includes additional agency response to our recommendations.[1] The work upon which this statement is based was conducted 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. More information on our scope and methodology can be found in our May 2016 report.[2]

[1]GAO, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy,* GAO-16-267 (Washington, D.C.: May 16, 2016).

[2]GAO-16-267.

Background

FBI's Use of Face Recognition Technology

For decades, fingerprint analysis has been the most widely used biometric technology for positively identifying arrestees and linking them with any previous criminal record. Beginning in 2010, the FBI began incrementally replacing the Integrated Automated Fingerprint Identification System (IAFIS) with Next Generation Identification (NGI) at an estimated cost of $1.2 billion.[3] 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 NGI 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 about 30 million photos to support criminal investigations.[4]

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.[5] 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.[6] Figure

[3]IAFIS was a national, computerized system for storing, comparing, and exchanging fingerprint data in a digital format. The FBI expects to complete the last NGI increment by 2017.

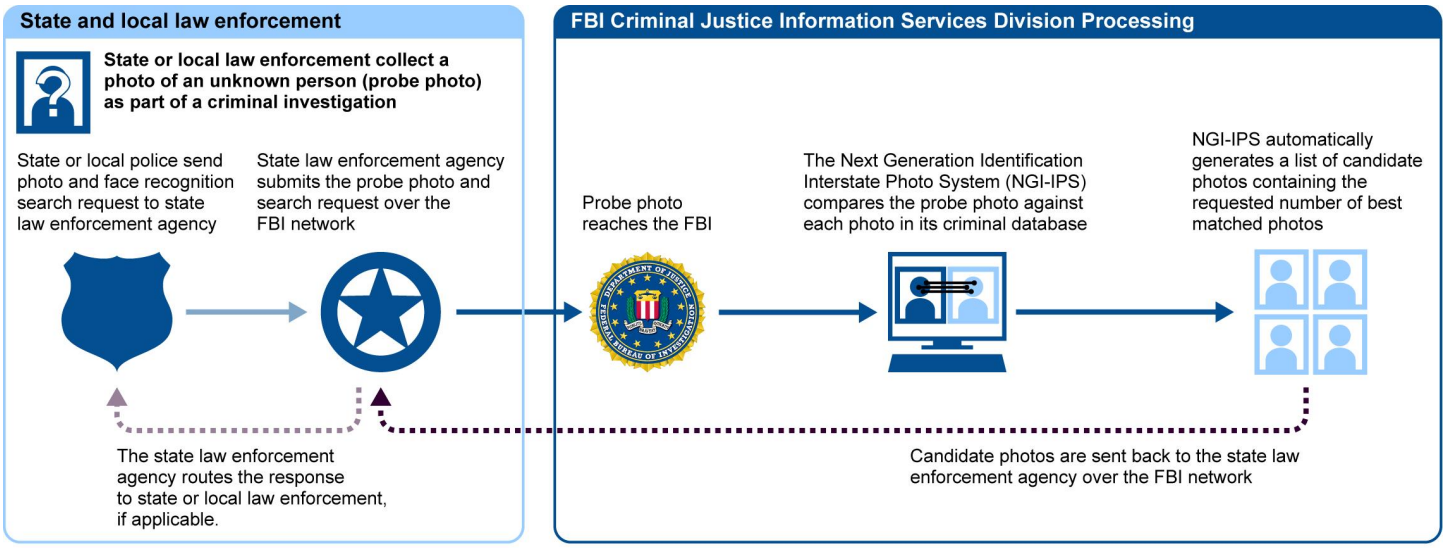
[4]The 30 million photos in NGI-IPS represent about 16.9 million individuals and reflect figures as of December 2015. When the FBI implemented IAFIS in 1999, the Criminal Justice Information Services (CJIS) Division began storing mugshots submitted with fingerprints in a photo database and also digitized all previously submitted hardcopy mugshots. However, until the implementation of NGI, users could only search for photos using the person's name or unique FBI number.

[5]The FBI began a pilot of NGI-IPS in December 2011, and NGI-IPS became fully operational in April 2015.

[6]We reported in May 2016 that as of December 2015, the FBI had agreements with 7 states to search NGI-IPS, and was working with more states to grant access. At the time of our review, FBI officials stated that the FBI did not offer this service to other federal agencies.

1 describes the process for a search requested by state or local law enforcement.

Figure 1: Description of the Federal Bureau of Investigation's (FBI) Face Recognition System Request and Response Process for State and Local Law Enforcement



Source: GAO analysis of FBI documentation. | GAO-17-489T

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.[7] 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.[8] Figure 2 shows which states partnered with FBI for FACE Services requests, as of August 2016. Unlike NGI-IPS, which primarily contains criminal photos, these external systems primarily contain civil photos from state and federal government databases, such as driver's

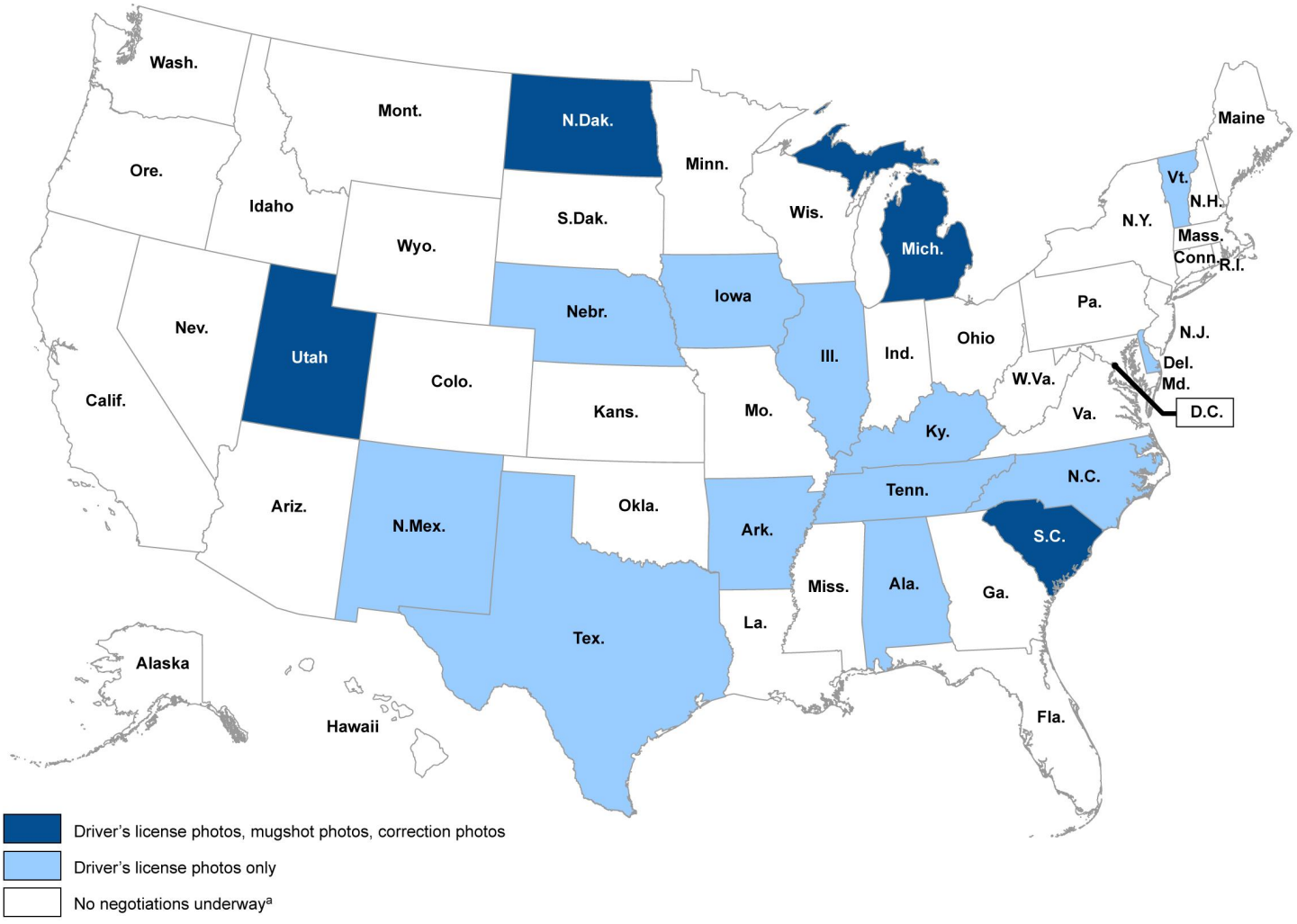
[7]FACE Services began supporting investigations in August 2011.

[8]According to FBI officials, the external photo databases do not contain privately obtained photos or photos from social media, and the FBI does not maintain these photos. Also, according to FBI officials, legal authority exists for the face recognition searching of all of these photo databases. For example, FBI officials 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 memorandums of understanding (MOUs) with their partner agencies that describe the legal authorities that allow the FBI to search the partner agencies' photos.

license photos and visa applicant photos. The total number of face photos available in all searchable repositories for FACE Services is over 411 million, and the FBI is interested in adding additional federal and state face recognition systems to its search capabilities.[9] Biometric images specialists for FACE Services manually review candidate photos from their external partners before returning at most the top 1 or 2 photos as investigative leads to the requesting FBI agents. However, 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.

[9]The over 411 million refers to photos, not identities and reflects data as of December 2015.

Figure 2: Information Available for the Federal Bureau of Investigation (FBI) Facial Analysis, Comparison, and Evaluation (FACE) Services' Photo Searches, by State



Source: GAO analysis of FBI information; Map Resources (map). | GAO-17-489T

[a]Some state laws prohibit face recognition.

Privacy Laws

Federal agency collection and use of personal information, including face images, is governed primarily by two laws: the Privacy Act of 1974[10] and the privacy provisions of the E-Government Act of 2002.[11]

- 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 system of records notice (SORN) in the Federal Register.[12] According to the Office of Management and Budget (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 Privacy Act.[13]
- The E-Government Act of 2002 requires that agencies conduct Privacy Impact Assessments (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.[14]

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

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

[12]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.; 5 U.S.C. 552a(a)(4)&(5).

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

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

DOJ and FBI Did Not Provide Timely Transparency and Have Not Fully Implemented Recommendations to Protect Privacy

DOJ Has an Oversight Structure in Place to Protect Privacy, but Did Not Publish Required Notices in a Timely Manner

Within the Department of Justice (DOJ), preserving civil liberties and protecting privacy is a responsibility shared by department level offices and components. As such, DOJ and the FBI have established oversight structures to help protect privacy and oversee compliance with statutory requirements. For example, while the FBI drafts privacy documentation for its face recognition capabilities, DOJ offices review and approve key documents developed by the FBI—such as PIAs and SORNs. However, the FBI did not update the NGI-IPS PIA in a timely manner when the system underwent significant changes and did not develop and publish a PIA for FACE Services before that unit began supporting FBI agents. Additionally, DOJ did not publish a SORN that addresses the collection and maintenance of photos accessed and used through the FBI's face recognition capabilities until after our 2016 review.

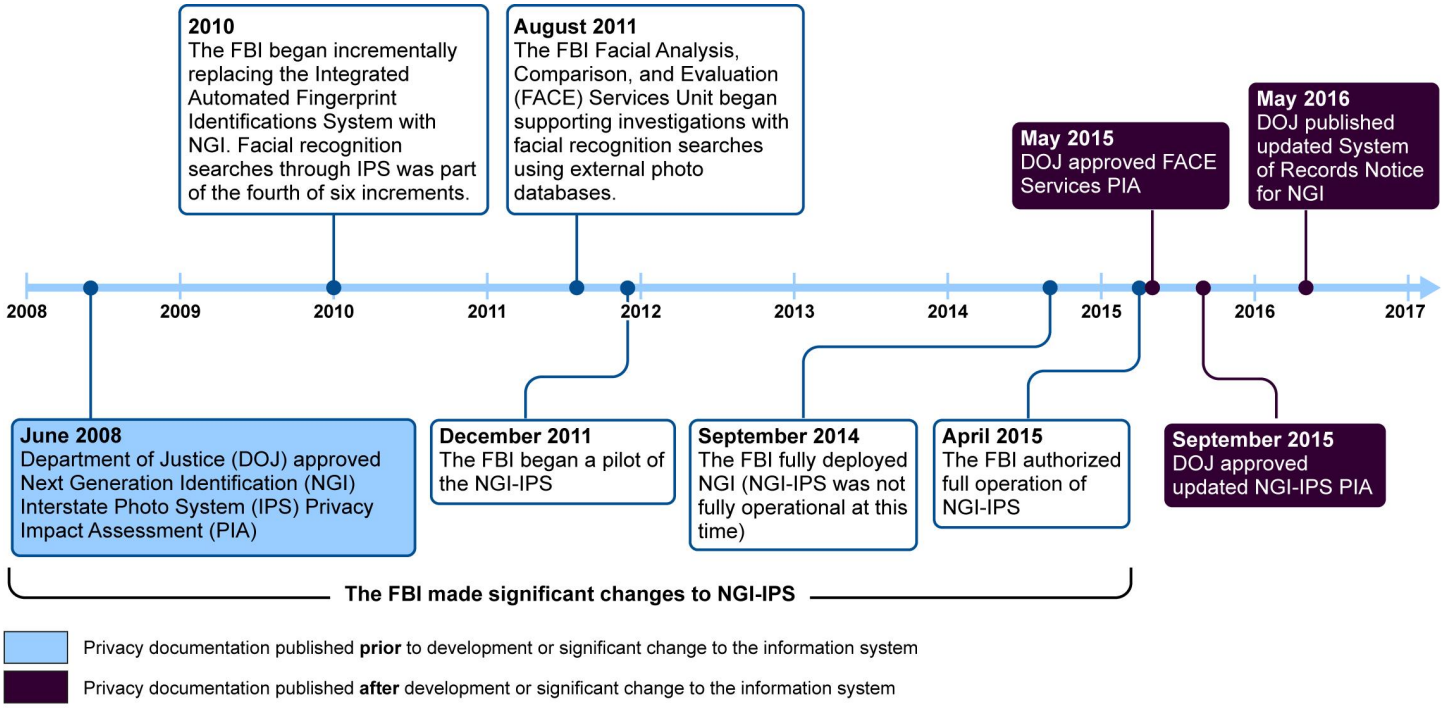
Consistent with the E-Government Act and OMB guidance, DOJ developed guidance that requires initial PIAs to be completed at the beginning of development of information systems and any time there is a significant change to the information system in order to determine whether there are any resulting privacy issues. DOJ published a PIA at the beginning of the development of NGI-IPS in 2008, as required.[15] However, the FBI did not publish a new PIA or update the 2008 PIA before beginning to pilot NGI-IPS in December 2011 or as significant changes were made to the system through September 2015.[16] During that

[15]Specifically, in 2008 the FBI published a PIA of its plans for NGI-IPS and indicated it was in the study phase, which included development of functional and system requirements.

[16]In December 2011, as part of a pilot program, the FBI began incrementally allowing a limited number of states to submit face recognition searches against a subset of criminal images in the FBI's database. Beginning in April 2015, states started transitioning from the pilot to full operational capability.

time, the FBI used NGI-IPS to conduct over 20,000 searches to assist in investigations throughout the pilot. Similarly, DOJ did not approve a PIA for FACE Services when it began supporting investigations in August 2011. As a new use of information technology involving the handling of personal information, it too, required a PIA.[17] Figure 3 provides key dates in the implementation of these face recognition capabilities and the associated privacy notices.

Figure 3: Key Dates in the Implementation of the Federal Bureau of Investigation's (FBI) Face Recognition Capabilities and Associated Privacy Impact Assessments and System of Records Notice



Source: GAO analysis of DOJ and FBI information. | GAO-17-489T

During the course of our review, DOJ approved the NGI-IPS PIA in September 2015 and the FACE Services PIA in May 2015—over three years after the NGI-IPS pilot began and FACE Services began supporting FBI agents with face recognition services. DOJ and FBI officials stated that these PIAs reflect the current operation of NGI-IPS and FACE Services. However, as the internal drafts of these PIAs were updated, the public remained unaware of the department's consideration for privacy

[17]The FBI conducted a privacy threshold assessment of FACE Services in 2012 that determined a PIA was necessary for the work log used to store personal information.

throughout development of NGI-IPS and FACE Services. This is because the updates were not published, as required.[18] 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.

Additionally, DOJ did not publish a SORN, as required by the Privacy Act, that addresses the collection and maintenance of photos accessed and used through the FBI's face recognition capabilities until May 5, 2016—after completion of our review. At that time, the FBI published a new SORN that reported the modification of the Fingerprint Identification Records System to be renamed the Next Generation Identification (NGI) System.[19] However, according to OMB guidance then in effect, the SORN must appear in the Federal Register before the agency begins to operate the system, e.g., collect and use the information.[20] 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. 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.

DOJ Disagrees with GAO's Recommendations regarding Privacy

In our May 2016 report, we made two recommendations to DOJ regarding its processes to develop privacy documentation, and DOJ officials disagreed with both. We recommended that DOJ assess the PIA development process to determine why PIAs were not published prior to using or updating face recognition capabilities. DOJ officials did not concur with this recommendation, and stated that the FBI has established practices that protect privacy and civil liberties beyond the requirements

[18]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.

[19]According to DOJ 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.

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

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 officials stated that it revised the FACE Services PIA as decisions were made. 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. In its response to our draft report, DOJ officials 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.

In March 2017, we followed up with DOJ to obtain its current position on our recommendation. DOJ continues to believe that its approach in designing the NGI system was sufficient to meet legal privacy requirements and that our recommendation represents a "checkbox approach" to privacy. We disagree with DOJ's characterization of our recommendation. We continue to believe that the timely development and publishing of future PIAs would increase transparency of the department's systems. We recognize the steps the agency took to consider privacy protection during the development of the NGI system. We also stand by our position that notifying the public of these actions is important and provides the public with greater assurance that DOJ components are evaluating risks to privacy when implementing systems.

We also recommended DOJ develop a process to determine why a SORN was not published 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. DOJ agreed, in part, with our recommendation and submitted the SORN for publication after we provided our draft report for comment. However:

- DOJ did not agree that the publication of a SORN is required by law. We disagree with DOJ's interpretation regarding the legal requirements of a SORN. The Privacy Act of 1974 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.[21] DOJ's 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.

- DOJ officials also stated that the FBI's face recognition capabilities do not represent new collection, use, or sharing of personal information. We disagree. 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. 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 personal information is being used and protected by DOJ components.

FBI Agreed to Conduct Audits to Oversee the Use of NGI-IPS and FACE Services

The Criminal Justice Information Services (CJIS), which operates FBI's face recognition capabilities, has 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. However, at the time of our review, it had not completed audits of the use of NGI-IPS or FACE Services searches of external databases. 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.[22] In addition, the FACE Services Unit has used external databases that include primarily civil photos to support FBI investigations since August 2011, but the FBI had not audited its use of these databases.[23] *Standards for Internal Control in the Federal Government* call for federal agencies to design and implement control activities to

[21]5 U.S.C. 552a(e)(4)(B).

[22]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.

[23]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.

enforce management's directives and to monitor the effectiveness of those controls.[24] In 2016, we recommended 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.

DOJ partially concurred with our recommendation. Specifically, DOJ concurred with the portion of our recommendation related to the use of NGI-IPS. DOJ officials stated that the FBI specified policy requirements with which it could audit NGI-IPS users in 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. As of March 2017, DOJ reported that the CJIS Audit Unit began assessing NGI-IPS requirements at participating states in conjunction with its triennial National Identity Services audit and that as of February 2017, the unit had conducted NGI-IPS audits of four states.

At the time we issued our 2016 report, DOJ officials did not fully comment on the portion of our recommendation that the FBI audit the use of external databases, because FBI officials said the FBI does not have authority to audit these systems. 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 and to ensure images are not disseminated for unauthorized purposes or to unauthorized recipients. In March 2017, DOJ provided us with the audit plan the CJIS Audit Unit developed in June 2016 for NGI-IPS users. DOJ officials said CJIS developed an audit plan of the FACE Services Unit to coincide with the existing triennial FBI internal audit for 2018. However, DOJ did not provide the audit plan for the FACE Services Unit. DOJ officials said the methodology would be the same as the audit plan for NGI-IPS, but that methodology does not

[24]9GAO, *Internal Control: Standards for Internal Control in the Federal Government,* GAO/AIMD-00-21.3.1 (Washington, D.C.: Nov. 1999).

describe oversight on use of information obtained from external systems accessed by FACE Services employees. Therefore, we believe DOJ is making progress towards meeting, but has not fully implemented our recommendation.

FBI Has Taken Limited Actions to Address Our Recommendations for Ensuring the Accuracy of its Face Recognition Capabilities

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

In May 2016, we reported that 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. However, the tests were limited because they did not include all possible candidate list sizes and did not specify how often incorrect matches were returned.[25] According to the National Science and Technology Council and the National Institute of Standards and Technology, 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) are both necessary to assess the accuracy of a face recognition system.[26] The FBI's detection rate requirement for face recognition searches 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). However, the FBI only tested this requirement with a candidate list of 50 potential matches. In these tests, according to FBI documentation, 86 percent of the time, a match to a person in the database was correctly returned. 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). As a result, we recommended that the FBI conduct tests of NGI-IPS to verify that the system is sufficiently accurate for all

[25]NGI-IPS automatically generates a list of candidate photos containing the requested number of best matched photos.

[26]National Science and Technology Council, *Biometrics Frequently Asked Questions* (Sept. 7, 2006) and National Institute of Standards and Technology, *Face Recognition Vendor Test: NIST Interagency Report 8009* (May 26, 2014).

allowable candidate list sizes and ensure that both the detection rate and the false positive rate are identified for such tests.

With the recommended testing, the FBI would have more reasonable assurance that NGI-IPS provides investigative leads that help enhance, rather than hinder or overly burden, criminal investigation work. If false positives are returned at a higher than acceptable rate, law enforcement users may waste time and resources pursuing unnecessary investigative leads. In addition, the FBI would help ensure that it is sufficiently protecting the privacy and civil liberties of U.S. citizens enrolled in the database. 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. [27] 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 comments on our draft report in 2016, and reiterated during recommendation follow-up, as of March 2017, DOJ did not concur with this recommendation. DOJ officials stated that the FBI has performed accuracy testing to validate 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. A key focus of our recommendation is the need to ensure that NGI-IPS is sufficiently accurate for all allowable candidate list sizes. 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. However, according to the FBI Information Technology Life Cycle Management Directive, testing needs to confirm the system meets all user

[27] *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).

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.

DOJ officials also stated that searches of NGI-IPS produce a gallery of likely candidates to be used as investigative leads, not for positive identification.[28] As a result, according to DOJ officials, NGI-IPS cannot produce false positives and there is no false positive rate for the system. We disagree with DOJ. The detection rate and the false positive rate are both necessary to assess the accuracy of a face recognition system. 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.

FBI Agreed to Conduct Annual Operational Reviews of NGI-IPS

FBI, DOJ, and OMB guidance all require annual reviews of operational information technology systems to assess their ability to continue to meet cost and performance goals.[29] 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, among other things. In 2016, we reported that the FBI had 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

[28]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.

[29]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).

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.[30] FBI's test database contains 926,000 photos while NGI-IPS contains about 30 million photos. As a result, we recommended the FBI 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.

In 2016, DOJ concurred with this recommendation. As of March 2017, FBI officials stated they implemented the recommendation by submitting a paper to solicit feedback from users through the Fall 2016 Advisory Policy Board Process. Specifically, officials said the paper requested feedback on whether the face recognition searches of the NGI-IPS are meeting their needs, and input regarding search accuracy.[31] According to FBI officials, no users expressed concern with any aspect of the NGI-IPS meeting their needs, including accuracy.

Although FBI's action of providing working groups with a paper presenting GAO's recommendation is a step, FBI's actions do not fully meet the recommendation. FBI's paper was presented as informational, and did not result in any formal responses from users. We disagree with FBI's conclusion that receiving no responses on the informational paper fulfills the operational review recommendation, which includes determining that NGI-IPS is meeting user's needs. As such, we continue to recommend the FBI conduct an operational review of NGI-IPS at least annually.

FBI Has Not Assessed the Accuracy of External Face Recognition Systems

In 2016 we reported that FBI officials did not assess the accuracy of face recognition systems operated by external partners. Specifically, before agreeing to conduct searches on, or receive search results from, these

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

[31]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.

systems, the FBI did not ensure the accuracy of these systems was sufficient for use by FACE Services. *Standards for Internal Controls in the Federal Government* call 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. As a result, we recommended the FBI 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.

In comments on our draft report in 2016, and reiterated during recommendation follow-up in 2017, DOJ officials did not concur with this recommendation. DOJ officials stated that the FBI has no authority to set or enforce accuracy standards of face recognition technology operated by external agencies. In addition, DOJ officials stated that the FBI has implemented multiple layers of manual review that mitigate risks associated with the use of automated face recognition technology. Further, DOJ officials stated there is value in searching all available external databases, regardless of their level of accuracy.

We disagree with the DOJ position. 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. We also disagree with the DOJ 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. 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. For example, the FBI's accuracy requirements for criminal investigative purposes may be different than a state's accuracy

requirements for preventing driver's license fraud.[32] 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. 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, whether the investment of public resources is justified, and whether photos of innocent people are unnecessarily included as investigative leads.

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, this concludes my prepared statement. I would be happy to respond to any questions you may have.

GAO Contact

For questions about this statement, please contact Diana Maurer at (202) 512-8777 or maurerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

Staff Acknowledgments

Individuals making key contributions to this statement include Dawn Locke (Assistant Director), Susanna Kuebler (Analyst-In-Charge), Jennifer Beddor, Eric Hauswirth, Richard Hung, Alexis Olson, and David Plocher. Key contributors for the previous work that this testimony is based on are listed in the previously issued product.

[32]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).

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, LinkedIn, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov and read The Watchblog.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548