Department of Justice

STATEMENT OF

KIMBERLY J. DEL GRECO
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON OVERSIGHT AND REFORM
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING CONCERNING

"THE USE OF FACIAL RECOGNITION TECHNOLOGY BY GOVERNMENT ENTITIES AND THE NEED FOR OVERSIGHT OF GOVERNMENT USE OF THIS TECHNOLOGY UPON CIVILIANS"

PRESENTED

JUNE 4, 2019

STATEMENT OF
KIMBERLY J. DEL GRECO
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON OVERSIGHT AND REFORM
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING CONCERNING
"THE USE OF FACIAL RECOGNITION TECHNOLOGY BY GOVERNMENT ENTITIES AND THE NEED FOR OVERSIGHT OF GOVERNMENT USE OF THIS TECHNOLOGY UPON CIVILIANS"

PRESENTED
JUNE 4, 2019

Good afternoon Chairman Cummings, Ranking Member Jordan, and members of the committee. Thank you for the opportunity to appear before you today and update the Committee on the Federal Bureau of Investigation's ("FBI") use of facial recognition technology.

Facial recognition is a tool that, if used properly, can greatly enhance law enforcement capabilities and protect public safety, but if used carelessly and improperly, may negatively impact privacy and civil liberties. The FBI is committed to the protection of privacy and civil liberties when it develops new law enforcement technologies. At the FBI trust is mission critical. If we lose trust, it may diminish our ability to deploy potentially live saving technologies, and everyone will suffer. For the FBI protecting the privacy and civil liberties of the American people is part of our culture. This is why when the FBI developed the use of facial recognition technologies, it also pioneered a set of best practices, so that effective deployment of these technologies to promote public safety can take place without interfering with our fundamental values. I welcome the opportunity to correct misconceptions regarding the FBI's use of this important technology. Key points of the FBI's use of facial recognition include the following:

- FBI policy strictly governs the circumstances in which facial recognition tools may be utilized, including what probe images may be used.

- FBI uses facial recognition technology for law enforcement purposes with human review and additional investigation. The FBI's use of facial recognition produces a potential investigative lead and requires investigative follow-up to corroborate the lead before any action is taken.

- Every face query--including results received from our partners--is reviewed and evaluated by trained examiners at the FBI to ensure the results are consistent with FBI standards.

- The FBI is committed to ensuring that FBI facial recognition capabilities are regularly tested, evaluated, and improved. In addition to system testing, the FBI has partnered with NIST to ensure algorithm performance is evaluated.

I would like to open with a description of the FBI CJIS Division programs that use facial recognition technology to perform "one to many" searches for law enforcement purposes. They are (1) the FBI's Next Generation Identification ("NGI") System located at the FBI's Criminal Justice Information Services ("CJIS") Division, and (2) the Facial Analysis, Comparison, and Evaluation ("FACE") Services Unit located at the FBI CJIS Division.

It is important to mention that from a technical and information security perspective, facial recognition services operate as a subsystem within the NGI system. All NGI subsystems must follow federal security protocols and receive the appropriate security testing and authorization to operate ("ATO") within NGI's ATO boundary. All NGI and NGI subsystem data is encrypted at rest and in transit. The NGI received its ATO prior to initial deployment and has maintained authority to operate via multiple re-accreditation actions since initial deployment.

1. **The NGI System maintains a photograph repository that is known as the Interstate Photo System ("IPS").** In the NGI-IPS, all criminal mugshots are associated with criminal tenprint fingerprints and a criminal history record. The NGI-IPS allows automated FR searches by authorized local, State, tribal, and federal law enforcement agencies. The law enforcement agency submits a "probe" photo that is obtained pursuant to an authorized law enforcement investigation, to be searched against the mugshot repository. The NGI-IPS returns a gallery of "candidate" photos of 2-50 individuals (the default is 20). During the second step of the process, the law enforcement agencies then manually review the candidate photos and perform further investigation to determine if any of the candidate photos are the same person as the probe photo.

   The NGI-IPS *Policy Implementation Guide* has been made available to authorized law enforcement users who receive candidate photos from the Next Generation Identification-Interstate Photo System. The policy prohibits photos being provided as positive identification and photos cannot serve as the sole basis for law enforcement action. In addition, the FBI has promulgated policies and procedures that place legal, policy, training, and security requirements on the law enforcement users of the NGI-IPS, including a prohibition against submitting probe photos that were obtained in violation of the First or Fourth Amendments. It is important to note that the FBI does not retain the probe photos; the probes are searched and deleted. Therefore, the FBI uses the NGI-IPS solely as a repository of criminal mugshots that are submitted by law enforcement partners with fingerprints pursuant to arrest.

   The FBI manages the CJIS Division, Advisory Policy Board ("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 System, administered by the FBI's CJIS Division, and thereafter, making appropriate recommendations.

In December 2017, the FBI Director approved the APB recommendation that requires law enforcement users to have completed training prior to conducting facial recognition searches of the NGI-IPS. The training must be consistent with the "Guidelines and Recommendations for Facial Comparison Training to Competency," as outlined by the Facial Identification Scientific Working Group ("FISWG").[1] This document provides the recommended elements of training to achieve competency in facial comparisons.

I would like to point out that from Fiscal Year 2017 through April 2019, the FBI CJIS Division received 152,565 Facial Recognition Search ("FSR") Requests of the NGI-IPS repository from authorized law enforcement users. During that time, there have been no findings of civil liberties violations or evidence of system misuse.

2. **The FACE Services Unit** provides investigative lead support to the FBI Field Offices, Operational Divisions, and Legal Attaches by comparing the face images of persons associated with open assessments[2] and active FBI investigations[3] against face images available in State and federal facial recognition systems. In limited instances, the FACE Services Unit provides facial recognition support for closed FBI cases (e.g., missing and wanted persons) and may offer recognition support to federal partners. The FACE Services Unit only accepts probe photos that have been collected pursuant to applicable legal authorities as part of an authorized FBI investigation. Upon receipt of the photo or photos, the FACE Services Unit searches them using facial recognition software against databases authorized for use by the FBI, which results in a photo gallery of potential candidates. The FACE Services Unit performs manual comparisons of candidate photos against the probe photos to determine a candidate's value as an investigative lead. This service does not provide positive identification, but rather, an investigative lead and

---

[1]Facial Identification Scientific Working Group, https://fiswg.org/FISWG_Training_Guidelines_Recommendations_v1.1_2010_11_18.pdf. The document provides guidance on the relevant subject matter to the individual so that upon the completion of training, they will be able to conduct comparisons at the basic level or at the advanced level.

[2]Per the Domestic Investigations and Operations Guide ("DIOG"), Section 5.4.1 Assessment Types and Section 5.5 Standards for Opening or Approving an Assessment, updated 12/28/18 - Assessments may be opened to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security.

[3]Per the DIOG, Section 6 Preliminary Investigations - Preliminary Investigations may be opened on the basis of "allegation or information" indicative of possible criminal activity or threats to national security. Full investigations may be opened when there is "an articulable factual basis" of possible criminal or national security threat activity.

analysis results that are returned to the FBI agent in the form of a "most likely candidate." The FBI agent must perform additional investigation to determine if the results provided by the FACE Services Unit is the same person as the probe photo.

The FBI FACE Services Unit has performed 390,186 searches on a variety of databases only in support of active FBI investigations with no findings of civil liberties violations or evidence of system misuse validated by the audit completed on December 17, 2018.

In performing the facial recognition searches, the FACE Services Unit operates under the authority of 28 U.S.C. §§ 533 and 534; 28 C.F.R. § 0.85; 42 U.S.C. § 3771; 18 U.S.C. Chapter 123, and the Driver Privacy Protection Act, 18 U.S.C. § 2721(b)(1). The FACE Services Unit performs facial recognition searches of FBI databases (e.g., FBI's NGI-IPS), other federal databases (e.g., Department of State's Visa Photo File, Department of Defense's Automated Biometric Identification System, Department of State's Passport Photo File), and State photo repositories (e.g., select State Departments of Motor Vehicles, criminal mugshots, corrections photos, etc.). Memoranda of Understanding and agreements have been established and are in place with all partners. The trained specialists in the FBI FACE Services Unit conduct multiple layers of manual review to mitigate risks.

Privacy Impact Assessments ("PIAs") for the FACE Services Unit and the NGI-IPS have been prepared by the FBI, approved by the Department of Justice ("DOJ"), and posted at https://www.fbi.gov/foia/privacy-impact-assessments. These PIAs provide to the public 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 civil liberties. The PIAs also reflect many of the privacy and civil liberties choices made during the implementation of these programs. The NGI System of Records Notice ("SORN"), *FBI-009 – The Next Generation Identification (NGI) System*, also discusses the use of FR technology and is posted in the Federal Register. See 81 FR 27283 (5-5-2016) at https://www.govinfo.gov/content/pkg/FR-2017-05-25/pdf/2017-10781.pdf and 82 FR 24151, 156 (5-25-2017) at https://www.govinfo.gov/content/pkg/FR-2017-05-25/pdf/2017-10781.pdf.

The FBI has made significant accuracy advancements with our research partners. At the end of 2017, the FBI finished an internal test of the NGI-IPS algorithm to validate the quoted accuracy of 85%. In 2018, the FBI partnered with the NIST to perform the Facial Recognition Vendor Test ("FRVT"). Results for algorithms submitted to NIST in February and June 2018 are published as NIST Interagency Report 8238; currently available online at www.NIST.gov . The report details recognition accuracy for 127 algorithms from 45 developers. From this test, the FBI determined a best-fit solution to upgrade its current NGI-IPS algorithm. The selected vendor's facial recognition algorithm boasted a Rank 1 accuracy of 99.12% and a Rank 50 accuracy of 99.72%.

Exercising due diligence and leveraging NIST results, the FBI announced on February 25, 2019 that the CJIS Division received authorization to proceed with an facial recognition

algorithm upgrade from the selected vendor as the best cost solution within the current FBI contract. The new facial recognition algorithm will increase the existing NGI-IPS facial recognition accuracy rate substantially. Following receipt of this new algorithm, the NGI System engineering and architecture team began developing the necessary system changes to support the new facial recognition algorithm and are more than 60% complete on the development environment. Following completion of the framework, the FBI CJIS Division will then perform software development updates, integration and testing, and recharacterization of current facial recognition algorithm templates into new NGI-IPS templates. The new facial recognition algorithm will be operational later towards the end of 2019 and is a high priority for the FBI CJIS Division.

Looking to the future, the FBI, in collaboration with the NIST, will be deploying "FRVT Ongoing" as early as summer 2019. "FRVT Ongoing" will enable the FBI to test its actual NGI-IPS facial recognition technology annually, as well as permit vendors to submit their facial recognition algorithms to NIST at least once a year. Traditionally, benchmark testing (such as FRVT 2018) is performed approximately every three or four years. However, due to the speed at which technology advances, traditional methods no longer permit the level of technology awareness the FBI desires. Therefore "FRVT Ongoing" will enable the FBI to comply with the Government Accountability Office ("GAO") and Congressional recommendations to perform annual testing, while also remaining acutely aware of technological advances within the facial recognition industry.

The FBI has submitted APB staff papers annually through the CJIS APB process to solicit feedback from its users on whether the facial recognition searches of the NGI-IPS are meeting their needs, specifically requesting input regarding search accuracy. To date, no users have expressed any concern with any aspect of the NGI-IPS meeting their needs, to include its accuracy. The APB is made up of 111 State, local, tribal, and territorial representatives, as well as a Federal Working Group, comprised of 23 representatives of federal agencies. The members represent approximately 18,000 law enforcement agencies from the 50 States, District of Columbia, U.S. Territories, and Canada. The FBI will continue to solicit input from the users regarding all FBI CJIS Systems including the NGI-IPS. Additionally, in December 2017, the FBI Director approved the APB recommendation to require CJIS Systems Agency/State Identification Bureau to provide training for individuals of agencies/States prior to conducting facial recognition searches of the NGI-IPS. Training must be consistent with the "Guidelines and Recommendations for Facial Comparison Training to Competency," as outlined by the Facial Identification Scientific Working Group.

The FBI FACE Services Unit performs "90-day call backs" to solicit feedback from FBI Agents that use the services provided by the FACE Services Unit. Their feedback enhances or improves the services offered by the FACE Services Unit and demonstrates a return on investment from the resulting stories and positive comments. To date, no FBI agents or staff have expressed concern regarding accuracy or performance issues.

It is important to note that the FBI has no authority to set or enforce accuracy standards of separate facial recognition technology operated by other agencies. The FBI CJIS Division agrees that accuracy and facial recognition system performance are important aspects of the overall management and efficacy of facial recognition technology. Based on its experience, the FBI CJIS Division believes that law enforcement and other government partners should also conduct reviews of their systems for accuracy and performance in order to protect privacy and civil liberties. The FBI CJIS Division understands the importance of the entire facial recognition community continuing to do so. While the FBI cannot direct partner actions to improve external facial recognition technology, the FBI recognizes the need to ensure that external facial recognition system capabilities meet or exceed the FBI's performance thresholds and works with partners to encourage performance enhancement wherever possible.

The FBI has implemented multiple layers of manual review by trained experts that mitigate risks associated with the use of automated facial recognition technology. Further, there is value in searching all available external databases, which have enabled the FBI to develop investigative leads, further investigations, and help solve crimes. As with the NGI-IPS, results returned to searches of external facial recognition systems are used as investigative leads and are not considered positive identifications. FBI agents using the services provided by the FACE Services Unit must make the final determination on the value of the facial recognition system responses relative to their investigation. These multiple levels of manual review minimize the risks associated with using automated facial recognition systems.

As facial recognition technology use expands, it is necessary for law enforcement, fusion centers, and other public safety agencies to ensure that comprehensive policies are developed, adopted, and implemented in order to guide the entity and its personnel in the day-to-day access and use of facial recognition technology. In 2017, the FBI went to the Criminal Intelligence Coordinating Council (CICC), a subcommittee of GLOBAL an Attorney General Federal Advisory Committee on Justice Information, to address this issue. GLOBAL and the CICC are under the oversight of the Bureau of Justice Assistance (BJA), a component of the Department of Justice. The CICC, with approval of GLOBAL and BJA, identified a priority to create a Global Facial Recognition Policy Development Template. This priority fell under the purview of the CICC since it is a state, local, tribal, and territorial focused law enforcement council whose purpose is to develop guidance and deliverables law enforcement entities.

To summarize, the NIST annual testing, in conjunction with the aforementioned training efforts, APB user feedback efforts, and collaboration opportunities are giving the FBI all the insight that it can reasonably attain in conducting an operational review of the NGI-IPS System on an annual basis.

The FBI performs audits as they serve an important role in identifying and mitigating risks associated with users of information systems not meeting policy requirements.

In March 2017, the FBI developed the triennial National Identity Services ("NIS") audit plan. Procedures for both external and internal NIS audits include review of NGI-IPS system transaction records and associated supporting documentation provided by audit participants. The FBI continues to conduct NIS audits of States enrolling and/or searching photos in the NGI-IPS, in conjunction with pre-established NIS triennial audits at State Identification Bureaus and federal agencies, and may include reviews at a selection of local agencies that access the NGI-IPS. Additionally, the NIS audit plan provides for an internal audit of the FBI FACE Services Unit to be conducted in accordance with existing procedures for FBI internal audits associated with CJIS system access. The FBI NIS established and provides the NIS Policy Reference Guide to each State for reference. This policy guide is a living document that includes all FBI CJIS policy and is revised and updated as necessary.

In September 2018, the FBI performed an audit on the FACE Services Unit to determine the extent to which users of the NGI-IPS and Biometric Images Specialists in the FACE Services Unit are conducting face images searches in accordance with privacy laws and CJIS policies. The audit evaluated processes and procedures implemented by the FACE Services Unit and included administrative review of a sample of NGI-IPS queries conducted by the FACE Services Unit to validate appropriate use of the system. The FBI concluded and documented in an FBI CJIS Internal FACE Services NIS Audit Report, dated December 17, 2018, that the FACE Services Unit is operating in accordance with privacy laws and FBI CJIS policies and made no recommendations.

As of May 2019, 14 States and the FACE Services Unit have connectivity with the NGI-IPS. To date, the FBI has conducted nine audits - there have been no findings of non-compliance, and no observations of unauthorized requests or misuse of the NGI-IPS identified during the NGI-IPS audits.

In closing, I would like to state that DOJ and the FBI CJIS Division have provided multiple and transparent status updates on all GAO and congressional inquiries relevant to the FBI's facial recognition technology.

The FBI's strength is directly attributable to the dedication of its people who work for and on behalf of their fellow citizens. Our adversaries and the threats we face are relentless. The FBI must continue to identify and use new capabilities such as automated facial recognition technology to meet the high expectations for the FBI to preserve our nation's freedoms, ensure our liberties are protected, and preserve our security. Quite simply put, we at the FBI cannot fail to meet our assigned mission. We must continue to exceed expectations and never rest on past successes. Hence, we must embrace new technologies such as automated facial recognition and optimize allocated resources to achieve mission objectives. At the same time, trust is mission critical. For this reason, the FBI has developed practices and procedures when it uses facial recognition technologies that constitute the state of the art in protecting privacy and civil liberties. I want to thank all of my colleagues for their support, and each employee at the FBI for their dedicated services. I am pleased to answer any questions you might have.