Billing Code: 4410-02-P

DEPARTMENT OF JUSTICE

28 CFR Part 16

[CPCLO Order No. 007-2017]

Privacy Act of 1974; Implementation

AGENCY: United States Department of Justice, Federal Bureau of Investigation.

ACTION: Final rule.

SUMMARY: The Federal Bureau of Investigation (FBI), a component of the United States Department of Justice (DOJ or Department), is issuing a final rule to amend its Privacy Act exemption regulations for the system of records titled, "Next Generation Identification (NGI) System," JUSTICE/FBI-009, last published in full on May 5, 2016. Specifically, the FBI exempts the records maintained in JUSTICE/FBI-009 from one or more provisions of the Privacy Act. The listed exemptions are necessary to avoid interference with the Department's law enforcement and national security functions and responsibilities of the FBI. This document addresses public comments on the proposed rule.

DATES: This final rule is effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT: Roxane M. Panarella, Assistant General Counsel, Privacy and Civil Liberties Unit, Office of the General Counsel, FBI, Washington DC, telephone 304-625-4000.

SUPPLEMENTARY INFORMATION:

Background

In 1990, the FBI published in the Federal Register a System of Records Notice (SORN) for the FBI system of records titled, "Identification Division Records System," JUSTICE/FBI-009. JUSTICE/FBI-009 evolved into the "Fingerprint Identification Records System (FIRS)," also referred to as the "Integrated Automated Fingerprint Identification System (IAFIS)," published at 61 FR 6386 (February 20, 1996), which covered individuals arrested or incarcerated, individuals applying for Federal employment or military service, registered aliens or naturalized citizens, and individuals wishing to place their fingerprints on record for personal identification purposes. The FIRS SORN included the following records:

A. Criminal fingerprint cards and/or related criminal justice information submitted by authorized agencies having criminal justice responsibilities;

B. Civil fingerprint cards submitted by Federal agencies and civil fingerprint cards submitted by persons desiring to have their fingerprints placed on record for personal identification purposes;

C. Identification records sometimes referred to as "rap sheets" which are compilations of criminal history information pertaining to individuals who have criminal fingerprint cards maintained in the system; and

D. A name index pertaining to all individuals whose fingerprints are maintained in the system.

As the system expanded, records continued to fall within the general categories of records specified in the SORN. As a policy matter, however, and in an effort to better detail the enhancements made to the system, the FBI and DOJ determined that

JUSTICE/FBI-009 should be modified to more fully describe the features and capabilities of the system, which has since been renamed the Next Generation Identification (NGI) System. Important enhancements to the NGI System include the increased retention and searching of fingerprints obtained for the purposes of licensing, employment, obtaining government benefits, and biometric services such as improved latent fingerprint searching and face recognition technology. Leading up to the publication of the modified SORN and a Notice of Proposed Rulemaking (NPRM) for the NGI System, the FBI conducted a series of Privacy Impact Assessments that detailed the steps taken by the FBI to fully assess the privacy impacts of new and modified NGI System components, addressing potential risks and mitigation techniques.

On May 5, 2016, the FBI issued a Notice of a Modified System of Records for the NGI System in the Federal Register at 81 FR 27284 (May 5, 2016), and an NPRM at 81 FR 27288 (May 5, 2016). In determining whether to claim exemptions, the FBI did not simply rely on exemptions granted to the predecessor system of records, but thoroughly evaluated the NGI System and its various components to determine whether exemptions were necessary. The necessary exemptions were proposed in the NPRM along with supporting rationales, and are to be codified in accordance with the issuance of this final rule.

Response to Public Comments

In its NGI System NPRM and Notice of a Modified System of Records, published on May 5, 2016, the Department invited public comment. The comment periods for both documents were originally set to close on June 6, 2016, but were extended 30 days to allow interested individuals additional time to analyze the proposal and prepare their

comments. The FBI received over 100 comments and letters from individuals, and from non-government, public interest, civil liberties, non-profit, and academic organizations. The FBI has closely reviewed and considered these comments. The following discussion is provided to respond to the NPRM comments and provide greater insight into the FBI's assessment of the need to claim exemptions from certain provisions of the Privacy Act for the NGI System.

Many questions and comments were received concerning the breadth and scope of the exemptions claimed. As noted in the NPRM and reiterated here, the following exemptions apply only to the extent information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j) or (k). Where compliance with an exempted section of the Privacy Act would not appear to interfere with or adversely affect the purposes of the NGI System to support law enforcement and to protect national security, the applicable exemption may be waived by the FBI in its sole discretion.

These exemptions are claimed with respect to the NGI System's records, which are compiled for the purposes of identifying criminal offenders or alleged criminal offenders, criminal investigations, and reports identifiable to an individual compiled throughout the criminal law enforcement process, including fingerprints, as well as associated biographic data, the nature and disposition of any criminal charges, and additional biometrics such as mugshots and palm prints, if available and if provided by the submitting agency. The NGI System records qualify for exemption from sections of the Privacy Act under 5 U.S.C. 552a(j)(2) because the FBI's principal function is the enforcement of criminal laws and the records maintained in the NGI System fall into one or more of the categories listed in (j)(2). Due to the evolving nature of identity records

and investigations and the scope of the NGI System, certain NGI System records may fall outside the scope of (j)(2) and would qualify for the specific exemptions under 5 U.S.C. 552a(k)(2) and (5). The exercise of all exemptions is discretionary and the FBI will not exercise an exemption of any section of the Privacy Act that is not appropriate and necessary.

5 U.S.C. 552a(c)(3), Accounting of Disclosures Upon Request of the Named Subject.

Some of the comments communicated concerns about claiming exemptions from accounting and audit disclosure requirements. As with exemptions claimed under subsections (c)(4) and (d), exemption from (c)(3) disclosure requirements is necessary to preserve the integrity of ongoing investigations. Revealing this information could compromise ongoing, authorized law enforcement and national security efforts by alerting an individual to collaborative law enforcement and national security investigations as well as the relative interests of the FBI and/or other investigatory agencies. Although the vast majority of NGI System disclosures need not be provided in an accounting request, the FBI must claim this additional exemption to ensure its ability to protect the integrity of ongoing investigations.

It is important to note that, despite claiming this exemption, the Privacy Act does not permit the FBI to exempt this system of records from the requirements codified under subsections 5 U.S.C. 552a(c)(1) and (c)(2). As a result, except under limited circumstances as outlined in the Privacy Act, the FBI is obligated to keep an accurate accounting of the date, nature, and purpose of each disclosure of a record maintained within this system of records, and retain the accounting for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made.

5 U.S.C. 552a(d)(1), (2), (3) and (4), (e)(4)(G) and (H), (e)(8), (f), Access to and Amendment of Records.

Many of the comments received concerned exemptions regarding the access to and amendment of records pursuant to 5 U.S.C. 552a(d)(1),(2),(3) and (4), (e)(4)(G) and (H), (e)(8), and (f). As with exemptions claimed to (c)(3) and (c)(4), providing access to these records could compromise ongoing investigations. It is necessary for the FBI to claim these exemptions because the NGI System also contains latent fingerprints, as well as other biometrics, and associated personal information that may be law enforcement or national security sensitive. Compliance with these provisions could alert the subject of an authorized law enforcement activity about that particular activity and the interest of the FBI and/or other law enforcement agencies. With that said, as cited in both the SORN and the NPRM, separate federal regulations (*see* 28 CFR 16.30–16.34 and 28 CFR 20.34) inform individuals of the process to access and amend their criminal history records in the NGI System. These regulations permit any person to receive his or her criminal history record for review and correction. If the individual has no criminal history record in the NGI System, he or she receives a letter confirming the absence of such record. Pursuant to the regulations, after an individual receives his or her criminal history record, he or she may consult both the FBI and the relevant criminal justice agency to correct or update the record. The vast majority of records in the NGI System have been entered by state and local law enforcement and require coordination with those agencies.

In addition, pursuant to 28 CFR 50.12, agencies submitting fingerprints to the FBI for individuals seeking employment, licensing, or similar benefits are required to inform

the applicants that their fingerprints will be searched in the NGI System and of the process for access and amendment under 28 CFR 16.30–16.34. The regulation also advises that agencies should afford the applicants the opportunity to correct or complete their records before making licensing or employment decisions. Additionally, for records claiming specific exemption under 5 U.S.C. 552a(k), if an individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, further access may be available.

Consequently, although the FBI has claimed exemptions to the notification, access, and amendment provisions of the Privacy Act for the NGI System, the FBI generally does not exercise these exemptions when doing so would not interfere with its law enforcement functions and responsibilities.

5 U.S.C. 552a(g), Rights of Judicial Redress.

The comments received also expressed concerns about the FBI's exemption from 5 U.S.C. 552a(g), which grants individuals the right to certain civil remedies under the Privacy Act. As a matter of clarification, the Privacy Act only permits an agency to exempt 5 U.S.C. 552a(g) if the records in the system of records qualify for the general exemption provisions under 5 U.S.C. 552a(j). This exemption cannot be, and has not been, claimed for the records within the NGI System that qualify for only the specific exemptions under 5 U.S.C. 552a(k).

Additionally, many comments expressed concern that by claiming an exemption from 5 U.S.C. 552a(g), the FBI would somehow absolve itself of meeting even those provisions of the Privacy Act that are not subject to exemption because an individual's right to seek a cause of action for any provisions of the Privacy Act would be exempted.

First, the FBI takes all of its constitutional and statutory requirements seriously, and does not limit its compliance to only those provisions of the Privacy Act subject to judicial redress. As addressed throughout this **SUPPLEMENTARY INFORMATION** section, even when an exemption is claimed, the FBI takes all reasonable and appropriate steps necessary to meet the requirements of the Privacy Act that would not interfere with its law enforcement functions and responsibilities. The FBI is subject to a number of oversight mechanisms to ensure compliance with its requirements under the Privacy Act, including internal and external audits and inspections.

Second, while the FBI has proposed an exemption from this provision for the NGI System, the exemption regulation is clear that the FBI will only claim exemptions to the extent that information in this system of records is subject to an exemption pursuant to the Privacy Act. Many courts have interpreted an agency's decision to exempt the Privacy Act's civil remedies provisions as only an exemption from a cause of action based on an exempted provision. In those jurisdictions, individuals are still permitted to exercise their right of judicial redress, pursuant to 5 U.S.C. 552a(g), for those provisions of the Privacy Act that are not subject to exemption.

5 U.S.C. 552a(e)(2), and (3), Collection Directly From the Individual.

Commenters also expressed concerns regarding the exemption from (e)(2) and (3) of the requirement to collect information directly from the individual.

The vast majority of the records in the NGI System are contributed by state and local law enforcement agencies. Because the FBI is neither the arresting official, nor the agency issuing the license, evaluating the individual for employment, or offering the benefit, it is impossible for the FBI to collect information directly from the subject.

However, in most circumstances these other agencies create the records using information obtained directly from the subject with his or her knowledge.

Fingerprints and other biometrics and information are collected by other government agencies based on their legal authorities to collect such information and submit it to the FBI. For records created for the purpose of licensing, employment, or to obtain a government benefit, the FBI requires that specific notice be provided to the applicant. This notice, in the form of a Privacy Act statement, discloses the authority which authorizes the solicitation of the information, whether disclosure of such information is mandatory or voluntary, the principal purpose for which the information is intended to be used, the routine uses which may be made of the information, and the effects on the individual, if any, of not providing all or any part of the requested information.

5 U.S.C. 552a(e)(4)(I), Categories of Sources of Records.

The FBI also received a comment concerning exemption of the requirement to disclose sources of records contained in the NGI System. Despite claiming this exemption, the FBI has published in the NGI SORN the categories of sources of records to the extent that such disclosure would not compromise confidential sources or the safety of witnesses. However, to the extent such additional details would be required, it is believed that such detail may interfere with the Department's law enforcement functions and the responsibilities of the FBI. The FBI claims the exemption to (e)(4)(I) because greater specificity than was provided in the NGI SORN cannot be disclosed without compromising confidential sources or the safety of witnesses.

5 U.S.C. 552a(e)(5), Accurate, Relevant, Timely, and Complete.

The comments also expressed concerns regarding the NGI System's exemption from the (e)(5) requirements to maintain accurate, relevant, timely, and complete records. When collecting information for authorized law enforcement purposes, it is not always possible to determine in advance what information is accurate, relevant, timely, or complete. With time, additional facts, and analysis, information may acquire new significance. Although the FBI has claimed this exemption, it continuously works with its federal, state, local, tribal, and international law enforcement partners to maintain the accuracy of records to the greatest extent possible. The FBI does so with established policies and practices that include the review, audit, and validation of records, and formal agreements with partner agencies that require regular records updates. The law enforcement and national security communities have a strong operational interest in using up-to-date and accurate records and will foster relationships with partners to further this interest. If alterations are made to criminal record sources outside the FBI, we encourage subject individuals to bring said documentation to the FBI's attention to ensure timely modification of an NGI System record.

General Comments on the NGI System.

A few commenters expressed concerns about the safety and security of the system. It should be noted that the FBI is not and cannot claim exemption from 5 U.S.C. 552a(e)(10), which requires agencies to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity. In compliance with this provision of the Privacy Act and other security mandates, the NGI System has been developed and implemented in compliance with all federal information

technology standards designed to safeguard personal information from loss, destruction, or unauthorized access.

Many commenters communicated concerns about the NGI System being used to track the expression of First Amendment rights. The NGI System is a biometric database. It is not utilized to conduct surveillance or track the expression of a citizen's First Amendment rights. It should be noted that the FBI is not and cannot claim exemption from 5 U.S.C. 552a(e)(7), which, absent specific authorization or consent, prohibits the maintenance of records describing how any individual exercises rights guaranteed by the First Amendment.

The FBI is not exempting the NGI System from all provisions of the Privacy Act. The protections of many of the provisions of the Privacy Act and the E-Government Act of 2002 are still in place; only the named Privacy Act exemptions have been claimed, if needed, to protect sensitive law enforcement and national security operations.

Overall, the FBI has made only minor, administrative edits to the rule as originally proposed to ensure accuracy and consistency with the listed authorities and other subsections of 28 CFR part 16. The FBI has made no substantive changes to the rule as it was originally proposed. For the reasons identified in this publication, the Department and the FBI are issuing this final rule.

List of Subjects in 28 CFR Part 16

Administrative practices and procedures, Courts, Freedom of information, Privacy Act.

Pursuant to the authority vested in the Attorney General by 5 U.S.C. 552a and delegated to me by Attorney General Order 2940-2008, 28 CFR part 16 is amended as follows:

Part 16—PRODUCTION OR DISCLOSURE OF MATERIAL OR INFORMATION

1. The authority citation for part 16 continues to read as follows:

Authority: 5 U.S.C. 301, 552, 552a, 553; 28 U.S.C. 509, 510, 534; 31 U.S.C. 3717.

Subpart E—Exemption of Records Systems Under the Privacy Act

2. Amend § 16.96 by revising paragraphs (e) and (f) to read as follows:

§ 16.96 Exemption of Federal Bureau of Investigation Systems – limited access.

* * * * *

(e) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4); (d)(1), (2), (3) and (4); (e) (1), (2) and (3); (e) (4) (G), (H) and (I); (e) (5) and (8); (f) and (g):

(1) The Next Generation Identification (NGI) System (JUSTICE/FBI-009).

(2) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j) or (k). Where compliance would not appear to interfere with or adversely affect the purpose of this system to detect, deter, and prosecute crimes and to protect the national security, the applicable exemption may be waived by the FBI in its sole discretion.

(f) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3), the requirement that an accounting be made available to the named subject of a record, because this system is exempt from the access provisions of subsection (d). Also, because making available to a record subject the accounting of disclosures from records concerning the subject would specifically reveal investigative interest by the FBI or agencies that are recipients of the disclosures. Revealing this information could compromise ongoing, authorized law enforcement and national security efforts and may provide the record subject with the opportunity to evade or impede the investigation.

(2) From subsection (c)(4) notification requirements because this system is exempt from the access and amendment provisions of subsection (d) as well as the accounting of disclosures provision of subsection (c)(3). The FBI takes seriously its obligation to maintain accurate records despite its assertion of this exemption, and to the extent it, in its sole discretion, agrees to permit amendment or correction of FBI records, it will share that information in appropriate cases.

(3) From subsection (d) (1), (2), (3) and (4), (e)(4)(G) and (H), (e)(8), (f) and (g) because these provisions concern individual access to and amendment of law enforcement records and compliance and could alert the subject of an authorized law enforcement activity about that particular activity and the interest of the FBI and/or other law enforcement agencies. Providing access could compromise sensitive law enforcement information, disclose information that would constitute an unwarranted invasion of another's personal privacy, reveal a sensitive investigative technique, provide information that would allow a subject to avoid detection or apprehension, or constitute a potential danger to the health or safety of law enforcement personnel, confidential

sources, or witnesses. Also, an alternate system of access has been provided in 28 CFR 16.30 through 16.34, and 28 CFR 20.34, for record subjects to obtain a copy of their criminal history records. However, the vast majority of criminal history records concern local arrests for which it would be inappropriate for the FBI to undertake correction or amendment.

(4) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary for law enforcement purposes. The relevance and utility of certain information may not always be evident until and unless it is vetted and matched with other sources of information that are necessarily and lawfully maintained by the FBI. Most records in this system are acquired from state and local law enforcement agencies and it is not possible for the FBI to review that information as relevant and necessary.

(5) From subsection (e)(2) and (3) because application of this provision could present a serious impediment to the FBI's responsibilities to detect, deter, and prosecute crimes and to protect the national security. Application of these provisions would put the subject of an investigation on notice of that fact and allow the subject an opportunity to engage in conduct intended to impede that activity or avoid apprehension. Also, the majority of criminal history records and associated biometrics in this system are collected by state and local agencies at the time of arrest; therefore it is not feasible for the FBI to collect directly from the individual or to provide notice. Those persons who voluntarily submit fingerprints into this system pursuant to state and federal statutes for licensing, employment, and similar civil purposes receive an (e)(3) notice.

(6) From subsection (e)(4)(I), to the extent that this subsection is interpreted to require more detail regarding the record sources in this system than has been published in the Federal Register. Should the subsection be so interpreted, exemption from this provision is necessary to protect the sources of law enforcement information and to protect the privacy and safety of witnesses and informants and others who provide information to the FBI.

(7) From subsection (e)(5) because in the collection of information for authorized law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With time, seemingly irrelevant or untimely information may acquire new significance when new details are brought to light. Additionally, the information may aid in establishing patterns of activity and providing criminal leads. Most records in this system are acquired from state and local law enforcement agencies and it would be impossible for the FBI to vouch for the compliance of these agencies with this provision. The FBI does communicate to these agencies the need for accurate and timely criminal history records, including criminal dispositions.

* * * * *

Dated: July 13, 2017.

Peter A. Winn,
Acting Chief Privacy and Civil Liberties Officer,
Department of Justice.

[FR Doc. 2017-15423 Filed: 7/31/2017 8:45 am; Publication Date: 8/1/2017]