Billing Code:4410-02-P

DEPARTMENT OF JUSTICE

28 CFR Part 16

[CPCLO Order No. 003-2020]

Privacy Act of 1974; Implementation

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

ACTION: Final rule.

SUMMARY: The Federal Bureau of lnvestigation (FBI), a component of the United States Department of Justice (DOJ or Department), is finalizing without changes its Privacy Act exemption regulations for the system of records titled, "National Crime Information Center (NCIC)," JUSTICE/FBI-001, which were published as a Notice of Proposed Rulemaking (NPRM) on September 18, 2019. Specifically, the Department's regulations will exempt the records maintained in JUSTICE/FBI-001 from one or more provisions of the Privacy Act. The exemptions are necessary to avoid interference with the FBI's law enforcement and national security functions and responsibilities. The Department received only one substantive comment 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: Katherine M. Bond, Assistant General Counsel, Privacy and Civil Liberties Unit, Office of the General Counsel, FBI, Washington DC, telephone 202-324-3000.

SUPPLEMENTARY INFORMATION: On September 10, 2019, the FBI published in the Federal Register a modified System of Records Notice (SORN) for an FBI system of records titled, "National Crime Information Center (NCIC)," JUSTICE/FBI-001, 84 FR 47533. The NCIC is a national criminal justice information system linking criminal (and authorized non-criminal) justice agencies located in the 50 states, the District of Columbia, U.S. territories and possessions, and selected foreign countries t.o facilitate the cooperative sharing of criminal justice information. The NCIC provides a system to receive and maintain information contributed by participating agencies relating to criminal justice and national security. Information maintained in the NCIC is readily accessible for authorized criminal justice purposes by authorized users via text-based queries (i.e., using names and other descriptive data).

On September 18, 2019, the FBI published a Notice of Proposed Rulemaking (NPRM) proposing to amend its existing regulations exempting records maintained in JUSTICE/FBI-001 from certain provisions of the Privacy Act pursuant to 5 U.S.C. 552aG) and (k), and inviting public comment on the proposed exemptions. 84 FR 49073. The comment period was open through October 18, 2019. DOJ received only one substantive comment responsive to the proposed exemptions. That comment, from the Electronic Privacy Information Center (EPIC), urged that "[a]ll of these proposals should be withdrawn," so that the Department claims no Privacy Act exemptions at all for NCIC system of records. EPIC makes a number of claims, among which are the following:

- "The over collection and maintenance of information that is unverified and unaccountable with no system for redress leaves personal data at a risk."

- "The FBI sets forward no reason that it should be able to maintain records irrelevant or unnecessary to accomplish a purpose of the agency."
- "[T]he categories of sources of records at minimum are essential in order to keep the government accountable throughout their data collection and law enforcement activities."
- "The exemptions as currently proposed are needlessly overbroad."
- "The NCIC has been known to have inaccurate and unreliable records, making it particularly unsuitable for vast exemptions from regulations designed to protect and optimize the accuracy and reliability of information held on people."

After consideration of the statements in this public comment from EPIC, the Department has determined that, to protect the ability of the FBI to properly engage in its law enforcement and national security functions, the exemptions as proposed in the NPRM are codified in this final rule for the reasons stated below.

Response to Public Comments

As stated above, the one substantive comment the FBI received regarding its NPRM urged the FBI to withdraw its proposed Privacy Act exemptions. While, generically, it might be true that "[t]he over collection and maintenance of information that is unverified and unaccountable with no system for redress leaves personal data at a risk," the Department does not agree with this characterization of the FBI's activities. Rather than "over collect," the FBI works with local, state, federal, and tribal criminal justice partners to determine what information is necessary to collect and share to ensure that the NCIC contains only information relevant and necessary to assist criminal justice agencies in fulfilling their missions. At times, due to the reality of law enforcement

investigations, it may not be possible to know in advance what information is relevant and necessary for law enforcement and intelligence purposes. That is one reason that Congress, in the Privacy Act, provided for the ability of agencies to exempt themselves from certain Privacy Act requirements.

Further, regarding the assertion that the FBI will be maintaining "unverified" information, NCIC policy includes strict validation requirements ensuring that criminal justice agencies periodically review their records to ensure to the extent feasible that they are accurate, timely, relevant, and complete. If a record is not timely validated, it is purged from the active NCIC file and retired. Additionally, NCIC policy requires that before any user can take official action on active records within the NCIC (e.g. arrest an individual, detain a missing person, seize stolen property, charge an individual with violation of a protection order, deny the purchase of a firearm, deny access to explosives), the user must confirm the validity and accuracy of the record with the agency that submitted the record to the NCIC. This ensures that agencies do not take action without verifying information from the NCIC. In addition, the FBI conducts triennial audits of all federal, state, and territorial repositories and a representative sample of local agencies to ensure compliance with policy. Findings of non-compliance are submitted to the Criminal Justice Information Services (CJIS) Advisory Policy Board for review. NCIC access is subject to termination for egregious violations of policy provisions. The NCIC also creates and maintains transaction logs, which can be reviewed to detect potential misuse of system data. And, regarding redress, the FBI in fact has had in place for many years a system for lawful access and amendment of records, detailed at 28 CFR part 16.

In the context of all of these steps taken by the FBI to promote data quality and appropriate data use, EPIC states that "NCIC has been known to have inaccurate and unreliable records"-citing its own past assertions as support for this statement-and concludes that EPIC's allegations make NCIC "particularly unsuitable for vast [Privacy Act] exemptions." When establishing the Privacy Act exemptions for law enforcement agencies, Congress considered and recognized the potential risks of law enforcement systems having inaccurate and unreliable records. Due to the nature of the type of work law enforcement agencies do and the type of information they must collect to do that work, it is not always possible to ensure the accuracy of records when collected. What is important is not whether a law enforcement agency may have inaccurate or unreliable records in its holdings; rather it is the steps taken by the law enforcement agency to promote data quality and appropriate data use under the circumstances. As detailed above, FBI efforts in this area are eminently reasonable, appropriate, and sufficient.

In response to EPIC's claim that "[t]he FBI sets forward no reason that it should be able to maintain records irrelevant or unnecessary to accomplish a purpose of the agency," the FBI has not made this claim. Nowhere does the FBI assert that it "should be able to maintain records irrelevant or unnecessary to accomplish a purpose of the agency." The FBI merely states the fact that it is a law enforcement agency and must act according to the realities and requirements of law enforcement investigations. As stated in the NPRM, relevance and necessity are questions of judgment and timing. Information that appears relevant and necessary when collected may, after further investigation and analysis, be deemed unnecessary. It is only after information is placed in the context of a

fully completed investigation and assessed in that light that its relevancy and necessity to a specific investigative activity can be established.

EPIC states that "the categories of sources of records at minimum are essential in order to keep the government accountable throughout their data collection and law enforcement activities." This statement fails to account for the wealth of public information,- including information published by the Department and FBI, detailing types of information maintained in the NCIC as well as indicating the state, local, federal, and tribal law enforcement agency contributors of that information. This plethora of publicly available information already exists and allows the public to keep the government accountable regarding this system of records. As information detailing sources becomes more discrete, however, the realities of law enforcement agencies and investigations again come into play, including the fact that information frequently comes from sensitive sources. As stated in the NPRM, should subsection (e)(4)(!) be interpreted to require more detail regarding the record sources in this system than has already been published in the Federal Register through the SORN documentation, exemption from this provision is necessary to protect the sources of law enforcement and intelligence information and to protect the privacy and safety of witnesses and informants and others who provide information to the FBI.

EPIC states that "[t]he exemptions as currently proposed are needlessly overbroad." On the contrary, in the NPRM and here in the Final Rule, the Department explains the need for each exemption. The exemptions as taken by FBI are as intended by Congress when it passed the Privacy Act, in order to ensure that law enforcement can continue to properly function in the face of the many requirements of the statute. After

careful consideration, Congress allowed for exemptions from some requirements and not from others. Rather than acting counter to the Privacy Act, the Department and FBI are acting pursuant to it. Further, even though the FBI is authorized under the Privacy Act to maintain certain exemptions in all cases, the FBI takes seriously the privacy interests of the public. As stated in the proposed rulemaking, where the FBI determines compliance with an exempted Privacy Act provision-including access and amendment provisions-would not appear to interfere with or adversely affect interests of the United States or other system stakeholders, the FBI at its sole discretion may waive such exemption in that circumstance in whole or in part. In each circumstance, the FBI considers whether the facts of the request merit compliance with an exempted Privacy Act provision(s). In appropriate circumstances, as indicated in the Final Rule, the FBI may waive such exemptions at its discretion.

The Department has considered the submitted comment; however, for the reasons set forth above and the rationales included in the regulations, the Department adopts in this Final Rule the exemptions and rationales proposed in the NPRM.

Executive Orders 12866 and 13563-Regulatory Review

This regulation has been drafted and reviewed in accordance with Executive Order 12866, "Regulatory Planning and Review" section l(b), Principles of Regulation, and Executive Order 13563 "Improving Regulation and Regulatory Review" section 1(b), General Principles of Regulation.

The Department of Justice has determined that this rule is not a "significant regulatory action" under Executive Order 12866, section 3(f), and accordingly this rule

has not been reviewed by the Office of Information and Regulatory Affairs within the Office of Management and Budget pursuant to Executive Order 12866.

Regulatory Flexibility Act

This regulation will only impact Privacy Act-protected records, which are personal and generally do not apply to an individual's entrepreneurial capacity, subject to limited exceptions. Accordingly, the Chief Privacy and Civil Liberties Officer, in accordance with the Regulatory Flexibility Act (5 U.S.C. 605(b)), has reviewed this regulation and by approving it certifies that this regulation will not have a significant economic impact on a substantial number of small entities.

Executive Order 13132 Federalism

This regulation will not have substantial direct effects on the States, on the relationship between the national government and the States, or on distribution of power and responsibilities among the various levels of government. Therefore, in accordance with Executive Order 13132, it is determined that this rule does not have sufficient federalism implications to warrant the preparation of a Federalism Assessment.

Executive Order 12988-Civil Justice Reform

This regulation meets the applicable standards set forth in sections 3(a) and 3(b)(2) of Executive Order 12988 to eliminate drafting errors and ambiguity, minimize litigation, provide a clear legal standard for affected conduct, and promote simplification and burden reduction.

Executive Order 13175-Consultation and Coordination with Indian Tribal Governments

This regulation will have no implications for Indian Tribal governments. More specifically, it does not have substantial direct effects on one or more Indian tribes, on the relationship between the Federal government and Indian tribes, or on the distribution of power and responsibilities between the Federal government and Indian tribes. Therefore, the consultation requirements of Executive Order 13175 do not apply.

Unfunded Mandates Reform Act of 1995

This regulation will not result in the expenditure by State, local and tribal governments, in the aggregate, or by the private sector, of $100,000,000, as adjusted for inflation, or more in any one year, and it will not significantly or uniquely affect small governments. Therefore, no actions were deemed necessary under the provisions of the Unfunded Mandates Reform Act of 1995.

Congressional Review Act

This rule is not a major rule as defined by 5 U.S.C. 804 of the Congressional Review Act.

Paperwork Reduction Act

This rule imposes no information collection or recordkeeping requirements.

List of Subjects in 28 CFR Part 16

Administrative practices and procedures, Courts, Freedom of information, and the 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.

2. Amend§ 16.96 by:

a. Revising paragraphs (g) and (h) and

b. Removing paragraph (i).

The revisions read as follows:

§ **16.96 Exemption of Federal Bureau of Investigation Systems-limited access.**

* * * * *

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

(I) National Crime Information Center (NCIC) (JUSTICE/FBI-001).

(2) These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552aG) and (k). Where the FBI determines compliance with an exempted provision would not appear to interfere with or adversely affect interests of the United States or other system stakeholders, the FBI in its sole discretion may waive an exemption, in whole or in part; exercise of this discretionary waiver prerogative in a particular matter shall not create any entitlement to or expectation of waiver in that matter or any other matter. As a condition of discretionary waiver, the FBI in its sole discretion may impose any restrictions deemed advisable by the FBI (including, but not limited to, restrictions on the location, manner, or scope of notice, access or amendment).

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

(I) 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 him/her would specifically reveal law enforcement or national security investigative interest in the individual by the FBI or agencies that are recipients of the disclosures. Revealing this information could compromise ongoing, authorized law enforcement and intelligence efforts, particularly efforts to identify and defuse any potential acts of terrorism or other potential violations of criminal law. Revealing this information could also permit the record subject to obtain valuable insight concerning the information obtained during any investigation and to take measures to circumvent the investigation (e.g., destroy evidence or flee the area to avoid 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 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), (e)(4)(G) and (H), (e)(8), (f), and (g) because these provisions concern individual access to and amendment of law enforcement and intelligence records and compliance could alert the subject of an authorized law

enforcement or intelligence activity about that particular activity and the investigative interest of the FBI and/or other law enforcement or intelligence agencies. Providing access could compromise sensitive law enforcement information; disclose information that could constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigative or intelligence 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, and witnesses. 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 with subjects of the information.

(4) From subsection (e)(l) because it is not always possible to know in advance what information is relevant and necessary for law enforcement and intelligence purposes. Relevance and necessity are questions of judgment and timing. For example, what appears rekvant and necessary when collected ultimately may be deemed unnecessary. It is only after information is assessed that its relevancy and necessity in a specific investigative activity can be established.

(5) From subsections (e)(2) and (3) because it is not feasible to comply with these provisions given the nature of this system. The majority of the records in this system come from other federal, state, local, joint, foreign, tribal, and international agencies; therefore, it is not feasible for the FBI to collect information directly from the individual or to provide notice. Additionally, the 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.

(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 already been published in the **Federal Register** through the SORN documentation. Should the subsection be so interpreted, exemption from this provision is necessary to protect the sources of law enforcement and intelligence information and to protect the privacy and safety of witnesses and informants and others who provide information to the FBI.

(7) From subsection (e)(S) because in the collection of information for authorized law enforcement and intelligence purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With time, additional facts, or analysis, information may acquire new significance. The restrictions imposed by subsection (e)(S) would limit the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement. Although the FBI has claimed this exemption, it continuously works with its federal, state, local, tribal, and international partners to maintain the accuracy of records to the greatest extent practicable. The FBI does so with established policies and practices. The criminal justice 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.

Dated: May 21, 2020

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

[FR Doc. 2020-11386 Filed: 6/23/2020 8:45 am; Publication Date: 6/24/2020]