Billing Code: 4410-09-P

DEPARTMENT OF JUSTICE

28 CFR Part 16

CPCLO Order No. 002-2013

Privacy Act of 1974; Implementation

AGENCY: Drug Enforcement Administration, United States Department of Justice.

ACTION: Final Rule.

SUMMARY: The Department of Justice (DOJ or Department), Drug Enforcement Administration (DEA) is issuing a final rule for the recently modified system of records titled "Investigative Reporting and Filing System" (IRFS), JUSTICE/DEA-008. This system, which has already been exempted from particular subsections of the Privacy Act of 1974, is now being exempted further. Information in this system relates to law enforcement and intelligence matters, and for the reasons set forth in the rule these exemptions are necessary to avoid interference with the law enforcement, counterterrorism, and national security functions and responsibilities of the DEA.

DATES: Effective [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT: DEA Headquarters, Attn: Bettie E. Goldman, Assistant Deputy Chief Counsel (CV), 8701 Morrissette Drive, Springfield, VA 22152, telephone 202-307-8040.

SUPPLEMENTARY INFORMATION:

Background

On April 11, 2012, the Department published an updated Privacy Act system of records notice (SORN) for IRFS at 77 FR 21808, a DEA system of records notice originally published on August 8, 1975, at 40 FR 38712. In conjunction with the IRFS SORN update, on April 18, 2012, the Department published a proposed rule at 77 FR 23173 to amend 28 CFR 16.98, which had established exemptions of IRFS from various Privacy Act provisions, as expressly authorized by Privacy Act subsections (j) and (k). The proposed rule did not significantly change the previously established exemptions of IRFS from Privacy Act subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (5), and (8); and (g). However, the proposed rule did add new exemptions of IRFS from Privacy Act subsections (e)(4)(G), (H), and (I); (f); and (h) and made general editorial revisions to the reasons for the existing IRFS exemptions. The public was provided with thirty (30) days in which to comment on the updated SORN and the proposed rule.

Public comments

The only comments the Department received with regard to the proposed rule were from the Electronic Privacy Information Center (EPIC).[1] The Department has carefully considered these comments but has declined to adopt them in the final rule. The Department has, however, added additional information in paragraphs 16.98(j)(9) and (11) of the final rule to provide greater clarity and help enhance public understanding of

[1] DOJ did not receive any comments directed at the updated IRFS SORN during the SORN comment period. EPIC's comments on the proposed rule did characterize the IRFS SORN as containing "a staggering twenty-seven routine uses" that EPIC perceived as presaging the disclosure of "troves of personally identifiable information to a seemingly endless list of recipients." To the extent that this might be deemed a general comment on the number and substance of the IRFS routine uses, the Department considers that these routine uses support disclosures that in appropriate circumstances are functionally equivalent to the purpose for which the information was collected or necessary and proper to the lawful furtherance of DEA's authorized mission functions. The Department also notes that many of these routine uses were in place before the most recent update to the SORN.

the reasons for these exemptions. A summary of EPIC's comments and the Department's responses are set forth below.

EPIC specifically noted five issues that it stated were raised by the proposed rule that EPIC considered to be substantial. In EPIC's opinion: (1) the proposed exemptions contravene the intent of the Privacy Act; (2) the DEA does not clearly articulate its legal authority to claim certain exemptions; (3) the DEA is required to collect only relevant and necessary information, and therefore, it should limit its information collection; (4) individuals within the IRFS system of records should have access to their information after criminal investigations are complete; and (5) individuals within the system should have a right to correct their information. Each of these contentions is separately discussed below.

(1) The proposed exemptions do not contravene the intent of the Privacy Act.

EPIC noted that IRFS may contain records about not only convicted drug offenders but also presumptively innocent individuals, such as those simply suspected of or alleged to have committed drug offenses. EPIC asserted that the "broad exemptions" established for IRFS would allow DEA employees to use sensitive information with little accountability and would contravene the intent of the Privacy Act.

The Privacy Act itself, specifically 5 U.S.C. 552a(j) and (k), authorizes DOJ to apply exemptions to IRFS. 5 U.S.C. 552a(j) states, "the head of any agency may promulgate rules . . . to exempt any system of records within the agency from any part of [the Privacy Act] except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i)." Similarly, Privacy Act subsection (k) expressly authorizes "[t]he head of any agency . . . [to] promulgate rules . . . to exempt any system of records within the

agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of [the Privacy Act]." Thus, DOJ's application of exemptions to IRFS is fully within the intent of the Privacy Act as it falls squarely within the statutory terms of the Act.

Further, applying exemptions to IRFS does not equate to DEA employees using IRFS "with little accountability." The DEA and its employees still must comply with important agency requirements in the Privacy Act that are not subject to exemption. For example, 5 U.S.C. 552a(j) lists the provisions of the Privacy Act from which the statute permits no exemption. In addition, as the proposed rule stated, exemptions apply only to the extent that information in the system is subject to the exemption.

The need for these exemptions exists even if a record subject may only be suspected of or alleged to have committed an offense, or may even be clearly innocent (such as victims or witnesses), because the reasons for these exemptions are present even if the individual may not be culpable. For example, disclosures to non-suspect individuals may present risks that the individual may either intentionally or accidently reveal the information to the suspect or to others involved in criminal activities or for whom disclosure would otherwise be inappropriate; may reveal sensitive investigative or intelligence techniques; may reveal classified information; may invade the privacy of third parties; or may otherwise prejudice investigative and adjudicative processes.

In addition, although the Department has exempted IRFS from subsection (e)(4)(1), the Department continues to describe the record source categories in order to provide greater public transparency. Withholding additional details 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 DEA; and

further, greater specificity of properly classified records could compromise national security. (The Department has added a discussion of this point in § 16.98(j)(9) of the final rule.) Finally, the Department again notes that most of these exemptions were in place prior to the notice of proposed rulemaking.

(2) DOJ has clear legal authority to establish these exemptions.

EPIC commented on DOJ's statutory authority to apply exemptions to IRFS, especially under subsection (k)(2), and questioned whether DOJ's application of exemptions is procedurally and substantively sound. As discussed above, the Privacy Act provides clear statutory authority for the exemptions DOJ is applying to IRFS,[2] the rule expressly provides that the exemptions will apply only to the extent that the IRFS information is subject to exemption, and the exemptions are justified for the reasons set forth in §16.98(j) of the rule. Further, DOJ has complied with procedural requirements to promulgate this rule.

The Department fully appreciates that exemption under (k)(2) generally does not permit an agency to deny an individual access to a record where the agency's maintenance of the record has resulted in the individual 'being denied a right, privilege, or benefit to which he or she would otherwise be entitled by Federal law, or for which he or she would otherwise be eligible. Subsection (k)(2) exemptions apply to investigatory material compiled for law enforcement purposes that is not otherwise subject to exemption under subsection (j)(2). The DEA is establishing (k)(2) exemptions in order to protect investigatory information that may not be subject to exemption under subsection (j)(2), as well as in circumstances where there is no issue relating to a denial of a right, privilege, or benefit.

[2] 5 U.S.C. 552a(j) and (k).

EPIC further objected to the provision in paragraph 16.98(i) of the rule that DEA may waive an applicable exemption in DEA's sole discretion. EPIC asserted that "it is not within the agency's sole discretion to waive an exemption if the exemption does not apply." As previously noted, the exemptions to IRFS only apply to the extent that information in this system is subject to exemption. If a record in IRFS is not subject to exemption under Privacy Act subsections (j)(2), (k)(1), or (k)(2), then the record will be subject to all pertinent Privacy Act provisions. It is only where a record is subject to an exemption that DEA would have the administrative discretion to waive an exemption in whole or in part.

(3) The scope of IRFS's information collection is necessary and specifically authorized by the Privacy Act.

EPIC's comments stated that the Privacy Act's "relevant and necessary" requirements were "designed to assure observance of basic principles of privacy and due process" and preclude arbitrary agency action. EPIC expressed the concern that government databases might become dossiers and be pressed into unintended uses ("mission creep"). EPIC suggested that, "[a]s investigations proceed to a close, information can be added or removed from the system as it becomes more or less relevant and necessary."

Both subsection (e)(1) and subsection (e)(5) are subject to exemption under subsection (j)(2), and subsection (e)(1) is also subject to exemption under subsection (k). As discussed in detail above, IRFS exemptions such as these are fully consistent with the language and intent of the Privacy Act, will apply only to the extent that the IRFS information is subject to exemption, and are justified for the reasons set forth in paragraph 16.98(j) of the rule. It is not always possible to know in advance what

information will turn out to be relevant or necessary, nor to know in advance whether information is accurate, timely, or complete. The process of conducting a law enforcement investigation involves the movement, in time, toward collection of relevant, necessary, accurate, timely, and complete information; however, it would be administratively impracticable for DEA to persistently add and remove information. The Privacy Act's exemption provisions strike the appropriate balance in anticipating and accommodating the law enforcement investigative process and administrative practicalities. This rule simply applies the law's provisions to help ensure the most effective and efficient accomplishment of DEA's statutory mission.

(4) Exempting IRFS from subsections (c)(3) and (e)(8) (and similar Privacy Act provisions) is necessary and specifically authorized by the Privacy Act.

EPIC's comments stated that DOJ should limit the extent of the (c)(3) and (e)(8) exemptions: "While EPIC recognizes the need to withhold notice during the period of the investigation, entities should be able to know, after an investigation is completed or made public, the information stored about them in the system."

The Privacy Act authorizes DOJ to exempt IRFS from subsections (c)(3) and (e)(8) under subsection (j)(2), and subsection (c)(3) is also subject to exemption under subsection (k). As discussed in detail above, these exemptions will apply only to the extent that the IRFS information is subject to exemption, and they are justified for the reasons set forth in paragraph 16.98(j) of the rule (e.g., because access to accounting of disclosures under subsection (c)(3) could impede or compromise an ongoing investigation, interfere with a law enforcement activity, lead to the disclosure of properly classified information which could compromise the national defense or disrupt foreign

policy, invade the privacy of a person who provides information in connection with a particular investigation, or result in danger to an individual's safety, including the safety of a law enforcement officer). Notice under subsection (e)(8) could impede criminal law enforcement by giving persons sufficient warning to evade investigative efforts, revealing investigative techniques, procedures, evidence, or interest, and interfering with the ability to issue warrants or subpoenas. In regard to subsection (e)(8), the Department would additionally note that investigations may still be ongoing even when related compulsory process becomes a matter of public record, and thus disclosures about related compulsory process may also have the same potentially adverse consequences explained in the proposed rule. Further, a necessity for DEA to monitor all instances of compulsory process involving IRFS records, to individually assess when each instance becomes a matter of public record, and to then provide notices to affected individuals would pose an impossible administrative burden on the maintenance of these records and the conduct of the underlying investigations. (The Department has added a discussion of this burden in §16.98(j)(11) of the final rule.)

In addition, pursuant to subsection (t)(2) of the Privacy Act, the Department cannot use Privacy Act exemptions established for IRFS as grounds to withhold from an individual any record which is otherwise accessible to such individual under the FOIA. To the extent that appropriately redacted IRFS records of completed investigations would not undermine law enforcement interests or invade the privacy of others, the individual may be able to obtain access to such records under the FOIA.

(5) Exempting IRFS from subsections (d)(2), (3), and (4) and (g) is necessary and specifically authorized by the Privacy Act.

EPIC objected to the Department's proposed exemption of IRFS from Privacy Act subsections (d)(2), (3), and (4) (which provide a process for individuals to seek and obtain correction of agency records about them), and from subsection (g) (which provides for judicial review of agency compliance with the Privacy Act). EPIC commented that individuals should be able to correct records about them because, "[i]ndividuals erroneously listed in the IRFS system of records can be subject to investigations by federal and local law enforcement agencies." EPIC also asserted that in proposing these exemptions the Department gave no consideration to the burdens placed on individuals from government agency misinformation. EPIC's comments also objected to exempting IRFS from subsection (g) because "individuals will have no judicially enforceable rights of access to their records or correction of erroneous information in such records."

Just as for the other exemptions that the Department proposed, Privacy Act subsections (d)(2), (3), and (4) and (g) are all subject to exemption under subsection (j)(2), and subsections (d)(2), (3), and (4) are also subject to exemption under subsection (k). IRFS exemptions such as these are thus fully consistent with the language and intent of the Privacy Act, will apply only to the extent that the IRFS information is subject to exemption, and are justified for the reasons set forth in § 16.98(j) of the rule. Further, contrary to EPIC's contention, in proposing these exemptions the Department did carefully consider the interests of the affected individuals. This consideration is reflected in the express notation in the proposed rule that, notwithstanding that the system may be exempted from a particular Privacy Act provision, where compliance with the provision would not appear to interfere with or adversely affect the law enforcement or counterterrorism purposes of this system, or the overall law enforcement process, the

DEA in its discretion may waive the exemption. The Department remains convinced that the proposed rule strikes the appropriate balance between the potential burdens the exemptions may place on individuals and the potential burdens the absence of exemptions may place on authorized law enforcement processes.

In sum, DOJ is adding a few new exemptions and making a few general revisions to its longstanding and existing IRFS exemptions, as permitted by the Privacy Act. The Department has carefully considered EPIC's comments, but declines to adopt them in the final rule.

List of Subjects in 28 CFR Part 16

Administrative practice and procedure, Courts, Freedom of information, Privacy, Sunshine 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—[AMENDED]

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

Authority: 5 U.S.C. 301, 552, 552a, 552b(g), 553; 18 U.S.C. 4203(a)(1); 28 U.S.C. 509, 510, 534; 31 U.S.C. 3717, 9701.

Subpart E – Exemption of Records Systems Under the Privacy Act

2. Amend § 16.98 by revising the section heading, paragraph (c), and paragraph (d) introductory text, and adding paragraphs (i) and (j) to read as follows:

§ 16.98 Exemption of Drug Enforcement Administration (DEA) Systems—limited access.

* * * * *

(c) Systems of records identified in paragraphs (c)(1) through (6) of this section are exempted pursuant to the provisions of 5 U.S.C. 552a (j)(2) from subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (5), and (8); and (g) of 5 U.S.C. 552a. In addition, systems of records identified in paragraphs (c)(1) through (5) of this section are also exempted pursuant to the provisions of 5 U.S.C. 552a(k)(1) from subsections (c)(3); (d)(1), (2), (3) and (4); and (e)(1):

(1) Air Intelligence Program (Justice/DEA-001).

(2) Clandestine Laboratory Seizure System (CLSS) (Justice/DEA-002).

(3) Planning and Inspection Division Records (Justice/DEA-010).

(4) Operation Files (Justice/DEA-011).

(5) Security Files (Justice/DEA-013).

(6) System to Retrieve Information from Drug Evidence (STRIDE/Ballistics) (Justice/DEA-014).

(d) Exemptions apply to the following systems of records only to the extent that information in the systems is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2): Air Intelligence Program (Justice/DEA-001); Clandestine Laboratory Seizure System (CLSS) (Justice/DEA-002); Planning and Inspection Division Records (Justice/DEA-010); and Security Files (Justice/DEA-013). Exemptions apply to the Operations Files (Justice/DEA-011) only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). Exemptions apply to the System to Retrieve Information from Drug Evidence (STRIDE/Ballistics) (Justice/DEA-014) only to the extent that information in the system is subject to exemption pursuant to

5 U.S.C. 552a(j)(2). Exemption from the particular subsections is justified for the following reasons:

* * * * *

(i) 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), (3), (4)(G), (H), (I), (5), and (8); (f); (g); and (h): Investigative Reporting and Filing System (IRFS) (JUSTICE/DEA-008). These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1), or (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement or counterterrorism purposes of this system, or the overall law enforcement process, the applicable exemption may be waived by the DEA in its sole discretion.

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

(1) From subsection (c)(3) because to provide a record subject with an accounting of disclosure of records in this system could impede or compromise an ongoing investigation, interfere with a law enforcement activity, lead to the disclosure of properly classified information which could compromise the national defense or disrupt foreign policy, invade the privacy of a person who provides information in connection with a particular investigation, or result in danger to an individual's safety, including the safety of a law enforcement officer.

(2) From subsection (c)(4) because this subsection is inapplicable to the extent that an exemption is being claimed for subsections (d)(1), (2), (3), and (4).

(3) From subsection (d)(1) because disclosure of records in the system could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation

of the existence of that investigation, of the nature and scope of the information and evidence obtained as to his activities, of the identity of confidential witnesses and informants, or of the investigative interest of the DEA; lead to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; reveal the details of a sensitive investigative or intelligence technique, or the identity of a confidential source; or otherwise impede, compromise, or interfere with investigative efforts and other related law enforcement and/or intelligence activities. In addition, disclosure could invade the privacy of third parties and/or endanger the life, health, and physical safety of law enforcement personnel, confidential informants, witnesses, and potential crime victims. Access to records could also result in the release of information properly classified pursuant to Executive order, thereby compromising the national defense or foreign policy.

(4) From subsection (d)(2) because amendment of the records thought to be incorrect, irrelevant, or untimely would also interfere with ongoing investigations, criminal or civil law enforcement proceedings, and other law enforcement activities; would impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised; and may impact information properly classified pursuant to Executive order.

(5) From subsections (d)(3) and (4) because these subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(6) From subsection (e)(1) because, in the course of its acquisition, collation, and analysis of information under the statutory authority granted to it, an agency may occasionally obtain information, including information properly classified pursuant to

Executive order, that concerns actual or potential violations of law that are not strictly within its statutory or other authority, or may compile information in the course of an investigation which may not be relevant to a specific prosecution. It is impossible to determine in advance what information collected during an investigation will be important or crucial to the investigation and the apprehension of fugitives. In the interests of effective law enforcement, it is necessary to retain such information in this system of records because it can aid in establishing patterns of criminal activity and can provide valuable leads for federal and other law enforcement agencies. This consideration applies equally to information acquired from, or collated or analyzed for, both law enforcement agencies and agencies of the U.S. foreign intelligence community and military community.

(7) From subsection (e)(2) because in a criminal investigation, prosecution, or proceeding, the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the investigation, prosecution, or proceeding would be placed on notice as to the existence and nature of the investigation, prosecution, and proceeding and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony. Moreover, thorough and effective investigation and prosecution may require seeking information from a number of different sources.

(8) From subsection (e)(3) because the requirement that individuals supplying information be provided a form stating the requirements of subsection (e)(3) would constitute a serious impediment to criminal law enforcement in that it could compromise

the existence of a confidential investigation or reveal the identity of witnesses or confidential informants and endanger their lives, health, and physical safety. The individual could seriously interfere with undercover investigative techniques and could take appropriate steps to evade the investigation or flee a specific area.

(9) From subsections (e)(4)(G) and (H) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act, and from subsection (e)(4)(I) to preclude any claims that the Department must provide more detail regarding the record sources for this system than the Department publishes in the system of records notice for this system. Exemption from providing any additional details about sources is necessary to preserve the security of sensitive law enforcement and intelligence information and to protect the privacy and safety of witnesses and informants and others who provide information to the DEA; and further, greater specificity of properly classified records could compromise national security.

(10) From subsection (e)(5) because the acquisition, collation, and analysis of information for criminal law enforcement purposes from various agencies does not permit a determination in advance or a prediction of what information will be matched with other information and thus whether it is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can often only be determined in a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators, intelligence analysts, and government attorneys to exercise their judgment in collating and analyzing

information and would impede the development of criminal or other intelligence necessary for effective law enforcement.

(11) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to criminal law enforcement by revealing investigative techniques, procedures, evidence, or interest, and by interfering with the ability to issue warrants or subpoenas; could give persons sufficient warning to evade investigative efforts; and would pose an impossible administrative burden on the maintenance of these records and the conduct of the underlying investigations.

(12) From subsections (f) and (g) because these subsections are inapplicable to the extent that the system is exempt from other specific subsections of the Privacy Act.

(13) From subsection (h) when application of this provision could impede or compromise an ongoing criminal investigation, interfere with a law enforcement activity, reveal an investigatory technique or confidential source, invade the privacy of a person who provides information for an investigation, or endanger law enforcement personnel.

Dated: **February 28, 2013.**

Joo Y. Chung
Acting Chief Privacy and Civil Liberties Officer
United States Department of Justice

[FR Doc. 2013-05146 Filed 03/06/2013 at 8:45 am; Publication Date: 03/07/2013]