Billing Code 4410-NW

DEPARTMENT OF JUSTICE

28 CFR Part 16

[CPCLO Order No. 002-2017]

Privacy Act of 1974; Implementation

AGENCY: United States Department of Justice.

ACTION: Notice of proposed rulemaking.

SUMMARY: Elsewhere in this Federal Register, the United States Department of Justice (Department or DOJ) has published a new Privacy Act System of Records Notice, JUSTICE/DOJ-018, "DOJ Insider Threat Program Records." Further, the Department issued a rescindment notice for the Federal Bureau of Investigation (FBI) System of Records Notice titled, "FBI Insider Threat Program Records," JUSTICE/FBI-023. In this document, the DOJ withdraws the notice of proposed rulemaking for the "FBI Insider Threat Program Records" issued in CPCLO Order No. 008-2016, published on September 19, 2016, and proposes to exempt JUSTICE/DOJ-018 from certain provisions of the Privacy Act, in order to avoid interference with efforts to detect, deter, and/or mitigate insider threats. Public comment is invited.

DATES: As of [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER], the notice of proposed rulemaking published at 81 FR 64092 (Sept. 19, 2016), is withdrawn. Comments on this notice of proposed rulemaking must be received by

[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Address all comments to the Privacy Analyst, Privacy and Civil Liberties Office, National Place Building, 1331 Pennsylvania Ave, NW, Suite 1000, Washington, DC 20530-0001, facsimile 202-307-0693, or email at privacy@usdoj.gov. To ensure proper handling, please reference the CPCLO Order No. of this notice of proposed rulemaking in your correspondence. You may review an electronic version of the proposed rule at *http://www.regulations.gov*, and you may also comment by using that website's comment form for this regulation. When submitting comments electronically, you must include the CPCLO Order No. in the subject box.

Please note that the Department is requesting that electronic comments be submitted before midnight Eastern Daylight Time on the day the comment period closes because *http://www.regulations.gov* terminates the public's ability to submit comments at that time. Commenters in time zones other than Eastern Time may want to consider this so that their electronic comments are received. All comments sent via regular or express mail will be considered timely if postmarked on or before the day the comment period closes.

Posting of Public Comments: Please note that all comments received are considered part of the public record and made available for public inspection online at *http://www.regulations.gov* and in the Department's public docket. Such information includes personal identifying information (such as your name, address, etc.) voluntarily submitted by the commenter.

If you want to submit personal identifying information (such as your name, address, etc.) as part of your comment, but do not want it to be posted online or made available in the public docket, you must include the phrase "PERSONALLY IDENTIFYING INFORMATION" in the first paragraph of your comment. You must also place all personal identifying information you do not want posted online or made available in the public docket in the first paragraph of your comment and identify what information you want redacted.

If you want to submit confidential business information as part of your comment, but do not want it to be posted online or made available in the public docket, you must include the phrase "CONFIDENTIAL BUSINESS INFORMATION" in the first paragraph of your comment. You must also prominently identify confidential business information to be redacted within the comment. If a comment has so much confidential business information that it cannot be effectively redacted, all or part of that comment may not be posted online or made available in the public docket.

Personally identifying information and confidential business information identified and located as set forth above will be redacted and the comment, in redacted form, will be posted online and placed in the Department's public docket file. Please note that the Freedom of Information Act applies to all comments received. If you wish to inspect the agency's public docket file in person by appointment, please see the "**FOR FURTHER INFORMATION CONTACT**" section, below.

FOR FURTHER INFORMATION CONTACT: Laurence Reed, DOJ Insider Threat Program Manager, United States Department of Justice, Insider Threat Prevention and

Detection Program, 145 N Street, NE, Washington, DC, 20002, 202-357-0165, itp@usdoj.gov.

SUPPLEMENTARY INFORMATION:

DOJ Insider Threat Program

The November 21, 2012, Presidential Memorandum – *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* states that an insider threat is the threat that any person with authorized access to any United States Government resources, to include personnel, facilities, information, equipment, networks or systems, will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

In the Notice section of this Federal Register, the DOJ has established a new Privacy Act system of records titled "DOJ Insider Threat Program Records," JUSTICE/DOJ-018. The system serves as a repository for DOJ information and for information lawfully received from other federal agencies or obtained from private companies and permits the comparison of data sets in order to provide a more complete picture of potential insider threats.

In this rulemaking, the DOJ proposes to exempt this Privacy Act system of records from certain provisions of the Privacy Act in order to avoid interference with the responsibilities of the DOJ to detect, deter, and/or mitigate insider threats as established by federal law and policy. For an overview of the Privacy Act, see: https://www.justice.gov/opcl/privacy-act-1974.

Integration of the FBI Insider Threat Program Records (ITPR) System of Records

On September 19, 2016, the Federal Bureau of Investigation (FBI), a component of the DOJ, published a new Privacy Act System of Records Notice titled, "FBI Insider Threat Program Records (ITPR)," JUSTICE/FBI-023, at 81 FR 64198. The FBI also issued a notice of proposed rulemaking, CPCLO No. 008-2016, at 81 FR 64092, proposing to exempt JUSTICE/FBI-023 from certain provisions of the Privacy Act. To consolidate Privacy Act notices under one DOJ-wide system of records, the Department is rescinding JUSTICE/FBI-023. In addition, the Department hereby withdraws the proposed rule, CPCLO No. 008-2016, published September 19, 2016, at 81 FR 64092, and will not publish a final rule to exempt JUSTICE/FBI-023 from certain provisions of the Privacy Act. Instead, the Department has published a new Privacy Act System of Records Notice titled, "DOJ Insider Threat Program Records," JUSTICE/DOJ-018, and proposes to exempt this DOJ-wide system of records from certain provisions of the Privacy Act, as described below.

Regulatory Flexibility Act

This proposed rule relates to individuals rather than small business entities. Pursuant to the requirements of the Regulatory Flexibility Act of 1980, 5 U.S.C. 601–612, therefore, the proposed rule will not have a significant economic impact on a substantial number of small entities.

Small Entity Inquiries

The Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996, 5 U.S.C. 801 *et seq*., requires the DOJ to comply with small entity requests for information and advice about compliance with statutes and regulations within DOJ jurisdiction. Any

small entity that has a question regarding this document may contact the person listed in the "**FOR FURTHER INFORMATION CONTACT**" section, above. Persons can obtain further information regarding SBREFA on the Small Business Administration's Web page at *http://www.sba.gov/advo/archive/sum_sbrefa.html*.

Paperwork Reduction Act

The Paperwork Reduction Act of 1995, 44 U.S.C. 3507(d), requires that DOJ consider the impact of paperwork and other information collection burdens imposed on the public. There are no current or new information collection requirements associated with this proposed rule. The records that are contributed to this system may be provided by individuals covered by this system, the DOJ and United States Government components, other domestic and foreign government entities, or purchased from private entities. Sharing of this information electronically will not increase the paperwork burden on the public.

Unfunded Mandates Reform Act of 1995

Title II of the Unfunded Mandates Reform Act of 1995 (UMRA), Public Law 103-3, 109 Stat. 48, requires Federal agencies to assess the effects of certain regulatory actions on State, local, and tribal governments, and the private sector. UMRA requires a written statement of economic and regulatory alternatives for proposed and final rules that contain Federal mandates. A "Federal mandate" is a new or additional enforceable duty, imposed on any State, local, or tribal government, or the private sector. If any Federal mandate causes those entities to spend, in aggregate, $100 million or more in any one year, the UMRA analysis is required. This proposed rule would not impose Federal mandates on any State, local, or tribal government or the private sector.

List of Subjects in 28 CFR Part 16

Administrative practices and procedures, Courts, Freedom of Information Act, 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 proposed to be 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, 553; 28 U.S.C. 509, 510, 534; 31 U.S.C. 3717.

Subpart E--Exemption of Records Systems Under the Privacy Act

2. Add § 16.137 to subpart E to read as follows:

§ 16.137 Exemption of the Department of Justice Insider Threat Program Records, JUSTICE/DOJ-018.

(a) The Department of Justice Insider Threat Program Records (JUSTICE/DOJ-018) system of records is exempted from subsections 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) of the Privacy Act. 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 DOJ determines compliance would not appear to interfere with or adversely affect the purpose of this system to detect, deter, and/or mitigate insider threats, the applicable exemption may be waived by the DOJ in its sole discretion.

(b) 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 of records concerning him/her would specifically reveal any insider threat-related interest in the individual by the DOJ 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/or mitigate insider threats. 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 impede the investigation, e.g., destroy evidence or flee the area to avoid 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 DOJ 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 DOJ 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, intelligence and counterintelligence, and counterterrorism records and compliance could alert the subject of an authorized law enforcement or intelligence

activity about that particular activity and the interest of the DOJ and/or other law enforcement or intelligence agencies. Providing access could compromise information classified to protect national security; disclose information that would 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, or witnesses.

(4) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary for law enforcement and intelligence purposes. The relevance and utility of certain information that may have a nexus to insider threats may not always be fully evident until and unless it is vetted and matched with other information necessarily and lawfully maintained by the DOJ.

(5) From subsection (e)(2) and (3) because application of these provisions could present a serious impediment to efforts to detect, deter and/or mitigate insider threats. Application of these provisions would put the subject of an investigation on notice of the investigation and allow the subject an opportunity to engage in conduct intended to impede the investigative 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 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 and intelligence information and to protect the privacy and safety of witnesses and informants and others

who provide information to the DOJ. Further, greater specificity of sources of properly classified records could compromise national security.

(7) From subsection (e)(5) because in the collection of information for authorized law enforcement and intelligence purposes, including efforts to detect, deter, and/or mitigate insider threats, due to the nature of investigations and intelligence collection, the DOJ often collects information that may not be immediately shown to be accurate, relevant, timely, and complete, although the DOJ takes reasonable steps to collect only the information necessary to support its mission and investigations. Additionally, the information may aid in establishing patterns of activity and providing criminal or intelligence leads. It could impede investigative progress if it were necessary to assure relevance, accuracy, timeliness and completeness of all information obtained throughout the course and within the scope of an investigation. Further, some of the records in this system may come from other domestic or foreign government entities, or private entities, and it would not be administratively feasible for the DOJ to vouch for the compliance of these agencies with this provision.

May 19, 2017
Date

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

[FR Doc. 2017-10788 Filed: 6/2/2017 8:45 am; Publication Date: 6/5/2017]