Billing Code: 4410-NW

DEPARTMENT OF JUSTICE

28 CFR Part 16

[CPCLO Order No. 008-2017]

Privacy Act of 1974; Implementation

AGENCY: United States Department of Justice.

ACTION: Final rule.

SUMMARY: 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, "DOJ Insider Threat Program Records," JUSTICE/DOJ-018. Specifically, DOJ is exempting the records maintained in JUSTICE/DOJ-018 from one or more provisions of the Privacy Act. The listed exemptions are necessary to avoid interference with efforts to detect, deter, and/or mitigate insider threats. This document addresses public comments on the proposed rule and codifies the claimed exemptions.

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

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:

Background

Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* (Oct. 7, 2011), requires the development of an executive branch program for the deterrence, detection, and mitigation of insider threats. The Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (Nov. 21, 2012), provides direction to executive branch departments on how to develop insider threat programs. The Presidential Memorandum states that an insider threat is the threat that any person with authorized access to any United States Government resource including 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 accordance with the Privacy Act of 1974 (Privacy Act), on June 5, 2017, DOJ issued a System of Records Notice (SORN) in the Federal Register at 82 FR 25812 (June 5, 2017), and a Notice of Proposed Rulemaking (NPRM) at 82 FR 25751 (June 5, 2017), for the "DOJ Insider Threat Program Records," JUSTICE/DOJ-018. The system establishes certain Department-wide capabilities to detect, deter, and mitigate insider threats, and will be used to facilitate management of insider threat inquiries and activities associated with inquiries and referrals, identify potential threats to DOJ resources and information assets, track referrals of potential insider threats to internal and external partners, and provide statistical reports and meet other insider threat reporting requirements. The system includes information provided by individuals covered by this

system and by DOJ. It may include information lawfully obtained by the DOJ from any United States Government entity, from other domestic or foreign government organizations, or from private entities, which is necessary to identify, analyze, or resolve insider threat matters. After consideration of public comments, exemptions necessary to safeguard this information and avoid interference with the responsibilities of DOJ to detect, deter, and/or mitigate insider threats are codified in this final rule.

Response to Public Comments

In its "DOJ Insider Threat Program Records" SORN and NPRM, published on June 5, 2017, the Department invited public comment. The period for public comment closed on July 5, 2017. The Department received one comment, which addressed elements of both the SORN and the NPRM. The Department has closely reviewed this comment and the following discussion responds to the comment.

The comment primarily focused on the scope of information collected by the system of records, the risk of compromise of such information, and the disclosures described in the SORN's "routine uses." As to the information collected by the system, the Department has determined that such information is necessary to create and maintain an effective insider threat program that complies with presidential mandates and federal law. The comment requests on page 7 that DOJ "maintain only records that are relevant and necessary to detecting and preventing inside threats," yet correctly points out on page 3 that the categories of records in the system include "relevant" counterintelligence and security databases and files, "relevant Unclassified and Classified network information," and "relevant Human Resources" databases and files. DOJ is a law enforcement agency. While it is not always possible to know in advance what information is relevant and

necessary for law enforcement and intelligence purposes, as explained further below, DOJ requires its employees and agents to take reasonable steps designed to ensure collection of relevant and necessary information.

As to the risk of compromise, DOJ understands the increase in data breaches across the public and private sectors. The Department has established appropriate administrative, technical and physical safeguards designed to ensure the security and confidentiality of records and to protect against anticipated threats or hazards to their security or integrity. The Department has implemented, and regularly assesses and works to strengthen, privacy and security controls required under federal law, regulations and policies, including the Federal Information Security Modernization Act of 2014, standards issued by the National Institute of Standards and Technology, and OMB guidelines (e.g., Circular A-130, Managing Information as a Strategic Resource). The Department's insider threat program is designed to minimize the risks of unauthorized disclosures of information, including a breach of personally identifiable information.

The Department has also determined that the disclosures described in the SORN's routine uses are necessary to create and maintain an effective insider threat program that complies with presidential mandates and federal law. In sum, the Department has thoroughly reviewed its program and determined that the SORN accurately describes the existence and character of the system of records, in accordance with the Privacy Act. For these reasons, no alterations will be made to the SORN and the system of records will operate in compliance with the representations made therein.

The comment also raised objections to some of the exemptions proposed in the NPRM. While the comment noted a general objection to claiming any of the exemptions

allowed under 5 U.S.C. 552a(j) and (k), specific objections were only raised for a few of the exemptions claimed regarding 5 U.S.C. 552a(e), detailing agency requirements. The Department addresses those objections in the following paragraphs.

5 U.S.C. 552a(e)(1), (d)(1)-(4), (e)(4)(G), (H), and (I), Relevant and Necessary, Notification, Access Procedures, Record Source Categories.

The comment asserted that the effect of claiming exemptions to 5 U.S.C. 552a(e)(1), (e)(4)(I), and (e)(4)(G) and (H) would be to diminish DOJ's legal accountability, stating that "DOJ claims the authority to collect any information it wants without disclosing where it came from or even acknowledging its existence." Contrary to the comment, the Department follows the letter and spirit of the Privacy Act in claiming these exemptions as a law enforcement and national security-focused agency. The Department maintains a constant commitment to protecting the privacy and civil liberties of all Americans.

Regarding 5 U.S.C. 552a(e)(1), the Department only collects information it is legally authorized to collect. Moreover, as explained below, 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 lawfully maintained by the DOJ. Nonetheless, DOJ requires its employees and agents to take reasonable steps designed to ensure collection of relevant and necessary information.

Regarding 5 U.S.C. 552a(e)(4)(I), the DOJ Insider Threat Program Records system of records notice disclosed to the greatest extent practicable the record source

categories for the information in the system. To the extent that Section 552a(e)(4)(I) is interpreted to require more detail regarding the record sources in this system than has already been published in the SORN, 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 Department.

The comment states that the Department is exempting itself from providing individuals access to and amendment of records in the system, which is under 5 U.S.C. 552a(d), and also implies the Department is exempting itself from providing notice to individuals regarding the procedures for access to and amendment of records, under 5 U.S.C. 552a(e)(4)(G) and (H). The Department proposed to exempt itself from the access and amendment requirements of 5 U.S.C. 552a(d)(1), (2), (3), and (4) because providing access and amendment rights to such records could compromise or lead to the compromise of 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; disclose or lead to disclosure of 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. Because the Department proposed to exempt itself from these access and amendment requirements, it logically follows that the Department also proposed to exempt itself from the requirement to publish notice to individuals of how to avail themselves of these access and amendment requirements under 5 U.S.C. 552a(e)(4)(G) and (H).

Nonetheless, in the SORN for the Insider Threat Program Records, DOJ provided notice of procedures to request access and amendment because, to the extent that an access or amendment request relates to information outside the scope of permissible exemptions, DOJ will comply with applicable requirements. Also, when DOJ compliance with an access or amendment request would not appear to interfere with or adversely affect the purpose of the system to detect, deter, and/or mitigate insider threats, the DOJ may waive the applicable exemption in its sole discretion and provide appropriate access or amendment.

5 U.S.C. 552a(e)(5), Accuracy, Relevance, Timeliness, and Completeness.

The comment asserts that the Department claiming an exemption to 5 U.S.C. 552a(e)(5), i.e., maintaining records "which are used by the agency in making any determination about an individual with such accuracy, relevance, timeliness, and completeness as reasonably necessary to assure fairness to the individual in the determination," means the Department "objects to guaranteeing 'fairness' to individuals in the 'Insider Threat' Database." The Department does not agree with this characterization. The collection of information for authorized law enforcement and intelligence purposes, including efforts to detect, deter, and/or mitigate insider threats, follows lawful, vetted investigative practices and procedures. In the investigative process, the DOJ at times collects information that may not be immediately shown to be accurate, relevant, timely, and complete. Law enforcement and intelligence investigators and analysts need to be able to collect the information they believe is necessary in their sound professional judgment to fully analyze a situation and move an investigation forward or close an investigation as appropriate. It could impede the investigative

process if DOJ were required to assure relevance, accuracy, timeliness and completeness of all information obtained throughout the course and within the scope of an investigation. Additionally, some of the records in this system may come from other domestic or foreign government organizations, or private entities, and it would not be administratively feasible for the DOJ to vouch for the compliance of these agencies with this provision. Understanding the inherent challenges in the investigative context that underlie DOJ's need to exempt this system from Privacy Act § 552a (e)(5), DOJ nonetheless requires and trains its personnel to take reasonable steps designed to ensure that records used by DOJ in making a determination about an individual are maintained with such accuracy, relevance, timeliness, and completeness as reasonably necessary to assure fairness to the individual in the determination.

The Department has concluded that, in light of the reasonable steps DOJ investigators and analysts are required to take in collecting and maintaining the information needed to support DOJ's mission and investigations, and in light of the compelling need to facilitate thorough and expeditious investigations and activities to deter, detect, and mitigate insider threats, exemption from the requirement of 5 U.S.C. 552a(e)(5) is appropriate for the Insider Threat Program Records System.

Conclusion

Because insiders have heightened access, and could potentially use that access, either wittingly or unwittingly, to do harm to the security of the United States, the Department must be particularly vigilant in its detection and investigation of insider threats. Nonetheless, the Department takes seriously its obligations to protect the privacy of Americans. As to the claimed exemptions, where DOJ determines that compliance

with an exempted Privacy Act provision would not appear to interfere with or adversely affect the purpose of this system to detect, deter, and/or mitigate insider threat, the applicable exemption may be waived by the Department in its sole discretion.

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

§ 16.137 Exemption of the Department of Justice Insider Threat Program Records—limited access.

(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 with these provisions 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 or lead to the compromise of 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; disclose or lead to disclosure of 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 DOJ in establishing patterns of activity and provide 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.

September 7, 2017
Date

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

[FR Doc. 2017-19483 Filed: 9/13/2017 8:45 am; Publication Date: 9/14/2017]