le: 4410-NW

DEPARTMENT OF JUSTICE

28 CFR Part 16

[CPCLO Order No. 010-2021]

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 finalizing without changes its Privacy Act exemption regulations for the system of records titled, Department of Justice Information Technology, Information System, and Network Activity and Access Records, JUSTICE/DOJ-002, which were published as a notice of proposed rulemaking (NPRM) (July 22, 2021). Specifically, the Department's regulations will exempt the records maintained in JUSTICE/DOJ-002 from one or more provisions of the Privacy Act. The exemptions are necessary to avoid interference with the efforts of DOJ and others to prevent the unauthorized access, use, disclosure, disruption, modification, or destruction of DOJ information and information systems, and to protect information on DOJ classified networks. The Department received no comments during the notice-and-comment period and is finalizing the rule without change.

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

FOR FURTHER INFORMATION CONTACT: Nickolous Ward, DOJ Chief Information Security Officer, (202) 514–3101, 145 N Street NE, Washington, DC 20530.

SUPPLEMENTARY INFORMATION: In accordance with the Federal Information Security Modernization Act of 2014, among other authorities, DOJ is responsible for complying with information security policies and procedures requiring information

security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of DOJ information and information systems. *See, e.g.*, 44 U.S.C. 3554 (2018). Consistent with these requirements, DOJ must ensure that it maintains accurate audit and activity records of the observable occurrences on its information systems and networks (also referred to as "events") that are significant and relevant to the security of DOJ information and information systems. These audit and activity records may include, but are not limited to, information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. Additionally, monitored events—whether detected utilizing information systems maintaining audit and activity records, reported to the Department by information system users, or reported to the Department by the cybersecurity research community and members of the general public conducting good faith vulnerability discovery activities—may constitute occurrences that (1) actually or imminently jeopardize, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitute a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. The Department has developed a formal process to track and document these reported "incidents," which may, in limited circumstances, include records of individuals reporting, or otherwise associated with, an actual or suspected event or incident.

In the Federal Register of July 14, 2021 (86 FR 37188), the Department modified a Department-wide system of records retitled, "Department of Justice Information Technology, Information System, and Network Activity and Access Records," JUSTICE/DOJ-002. This system of records covers the Department's tracking of all DOJ information technology, DOJ information system, and DOJ network activity and access by users. These records assist Department information security professionals in

protecting DOJ information, ensuring the secure operation of DOJ information systems, and tracking and documenting incidents reported to the agency. The revisions to this notice reflect changes in technology, including the increased ability of the Department to link individuals to information technology, information system, or network activity, and to better describe the Department's records linking individuals to reported cybersecurity incidents or their access to certain information technologies, information systems, and networks through the Internet or other authorized connections.

The Department received no comments in response to the NPRM for JUSTICE/DOJ-002 (86 FR 38624 (July 22, 2021)), and now finalizes this rule without changes. In this rulemaking, the Department exempts JUSTICE/DOJ-002 from certain provisions of the Privacy Act in order to avoid interference with the responsibilities of the Department to prevent the unauthorized access, use, disclosure, disruption, modification, or destruction of DOJ information and information systems. Additionally, the Department exempts JUSTICE/DOJ-002 from certain provisions of the Privacy Act to protect activity and audit log records on DOJ classified networks.

The Department notes that the name of the system of records which is the subject of this rule was changed from "Department of Justice Computer Systems Activity and Access Records" to "Department of Justice Information Technology, Information System, and Network Activity and Access Records" in the notice that was published on July 14, 2021. The NPRM, which was published on July 21, 2021, inadvertently referred to the system of records by the previous name. Additionally, the NPRM indicated in one place an exemption from subsection (d), and in another place an exemption from subsections (d)(1) – (4). In an effort to reduce potential confusion, the language in the final rule has been modified to consistently identify the system of records as being exempted from subsections (d)(1) – (4). Further, corrections have been inserted in the final rule in multiple places where the NPRM had used the term "system," although

"system of records" was clearly intended. Finally, the proposed rule stated that, in determining the relevance and utility of certain exempted information, it would be vetted and matched with other information necessarily and lawfully maintained by the DOJ, external federal agency subscribers, or other entities. Such information need only be maintained lawfully by the DOJ, external federal agency subscribers, or other entities for use in the vetting and matching described. The Department has determined that these changes do not significantly alter the efficacy of the notice that was provided to the public. The Department has made the adjustments in the final rule, which is published herein.

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 1(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.

Small Business Regulatory Enforcement Fairness Act of 1996 (Subtitle E–Congressional Review Act)

The Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996, 5 U.S.C. 801 *et seq.*, requires the Department to comply with small entity requests for information and advice about compliance with statutes and regulations within the Department's jurisdiction. Any small entity that has a question regarding this document may contact the person listed in FOR FURTHER INFORMATION CONTACT section, above. Persons can obtain further information regarding SBREFA on the Small Business Administration's web page at *https://www.sba.gov/advocacy.* 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, Privacy.

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, the Department of Justice amends 28 CFR part 16 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 § 16.138 to read as follows:

§ 16.138 Exemption of the Department of Justice Information Technology, Information System, and Network Activity and Access Records, JUSTICE/DOJ-002.

(a) The Department of Justice Information Technology, Information System, and Network Activity and Access Records (JUSTICE/DOJ-002) system of records is exempted from subsections (c)(3); (d)(1), (2), (3) and (4); (e)(1), (e)(4)(G), (H), and (I); and (f) of the Privacy Act of 1974, as amended. The exemptions in this paragraph (a) apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(1) or (k)(2). The applicable exemption may be waived by the DOJ in its sole discretion where DOJ determines compliance with the exempted provisions of the Act would not interfere with or adversely affect the purpose of this system of records to ensure that the Department can track information system access and implement information security protections commensurate with the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of DOJ information and DOJ information systems.

(b) Exemptions from the particular subsections listed in paragraph (a) of this section 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 of records is exempt from the access provisions of subsection (d). Also, because making available to a record subject the accounting of disclosures of records concerning the subject would specifically reveal investigative interests in the records by the DOJ or other entities that are recipients of the disclosures. Revealing this information could compromise sensitive information classified in the interest of national security, or interfere with the overall law enforcement process by revealing a pending sensitive cybersecurity investigation. 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 alter techniques to evade discovery.

(2) From subsection (d)(1), (2), (3) and (4), (e)(4)(G) and (H), and (f) because these provisions concern individual access to and amendment of records, compliance with which regarding certain law enforcement and classified records could alert the subject of an authorized law enforcement 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, or reveal sensitive cybersecurity investigative techniques; provide information that would allow a subject to avoid detection; or constitute a potential danger to the health or safety of law enforcement personnel or confidential sources.

(3) 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 cybersecurity threats may not always be fully evident until and unless it is vetted and matched with other information lawfully maintained by the DOJ or other entities.

(4) 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. Further, greater specificity of sources of properly classified records could compromise national security.

Dated: October 26, 2021.

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

[FR Doc. 2021-24315 Filed: 11/5/2021 8:45 am; Publication Date: 11/8/2021]