BILLING CODE: 7515-01U

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

36 CFR part 1202

[FDMS No. NARA-16-0005; NARA-2016-021]

RIN 3095-AB91

Privacy Act of 1974; Exemptions

AGENCY: National Archives and Records Administration (NARA).

ACTION: Direct final rule.

SUMMARY: The National Archives and Records Administration (NARA) is revising its Privacy Act regulations to add a new insider threat system of records to the records exempt from release under the law enforcement exemption of the Privacy Act. This action is necessary to protect investigatory information from release that could compromise or damage the investigation, result in evidence tampering or destruction, undue influence of witnesses, danger to individuals, and similar harmful effects.

DATES: This rule is effective [INSERT DATE 40 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], without further action, unless NARA receives adverse comments warranting action by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. If NARA receives an adverse comment warranting further action, it will publish a timely withdrawal of the rule in the Federal Register.

ADDRESSES: You may submit comments, identified by RIN 3095-AB91, by any of the following methods:

- *Federal eRulemaking Portal:* http://www.regulations.gov. Follow the instructions for submitting comments.

- *Email:* Regulation_comments@nara.gov. Include RIN 3095-AB91 in the subject line of the message.
- *Fax:* 301-837-0319. Include RIN 3095-AB91 in the subject line of the fax cover sheet.
- *Mail* (for paper, disk, or CD-ROM submissions. Include RIN 3095-AB91 on the submission): Regulations Comment Desk (External Policy Program, Strategy & Performance Division (SP)); Suite 4100; National Archives and Records Administration; 8601 Adelphi Road; College Park, MD 20740-6001
- *Hand delivery or courier:* Deliver comments to front desk at the address above.

Instructions: All submissions must include NARA's name and the regulatory information number for this rulemaking (RIN 3095-AB91). We may publish any comments we receive without changes, including any personal information you include.

FOR FURTHER INFORMATION CONTACT: Kimberly Keravuori, by email at regulation_comments@nara.gov, or by telephone at 301-837-3151.

SUPPLEMENTARY INFORMATION: The National Archives and Records Administration (NARA) is adding a system of records to its existing inventory of systems subject to the Privacy Act of 1974, as amended (5 U.S.C. 552(a)) ("Privacy Act"). The new system is NARA 45, Insider Threat Program records (we are publishing the NARA 45 SORN concurrently with this regulation), and it comprises records gathered for purposes of investigating threats to NARA facilities, personnel, or systems, or national security. The system contains investigatory material of actual, potential, or alleged criminal, civil, or administrative violations and law enforcement actions.

The Privacy Act generally grants individuals the right to access agency records maintained about themselves, and the right to request that the agency amend those records if they

are not accurate, relevant, timely, or complete. However, the Privacy Act also exempts, by means of ten specific exemptions, an agency from granting a person access to information about themselves that the agency compiles for certain types of law enforcement or investigatory actions. Specifically for the purposes of this rulemaking, the Privacy Act exempts an agency from granting access to "investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: provided, however, that if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section [September 27, 1975], under an implied promise that the identity of the source would be held in confidence." 5 U.S.C. 552a(k)(2).

NARA currently exempts Office of Inspector General investigative files under the (k)(2) exemption. See 36 CFR 1202.92. For similar reasons, we are now adding the insider threat program files to the same regulation section because the Insider Threat Program Records system of records contains investigatory material of actual, potential, or alleged violations, compiled for law enforcement purposes. Under Office of Management and Budget (OMB) Guidelines on the Privacy Act, to qualify for this exemption the agency must compile the material for some investigative "law enforcement" purpose, such as a civil or criminal investigation. Multiple court decisions have upheld the exemption for investigative records covering a range of purposes from discrimination complaints (see, e.g., Menchu v. HHS, 965 F. Supp. 2d 1238, 1248 (D. Or. 2013)), fraud, waste, and abuse complaints (see, e.g., Gowan v. Air Force, 148 F.3d 1182, 1188-

89 (10th Cir. 1998)), and taxpayer audits (see, e.g., Welsh v. IRS, No. 85-1024, slip op. at 2-3 (D.N.M. Oct. 21, 1986)), to civil trust fund recovery penalty investigations (see, e.g., Berger v. IRS, 487 F. Supp. 2d 482, 497-98 (D.N.J. 2007), aff'd288 F. App'x 829 (3d Cir. 2008), cert. denied, 129 S. Ct. 2789 (2009)) and deportation investigations (see, e.g., Shewchun v. INS, No. 95-1920, slip op. at 3, 8-9 (D.D.C. Dec. 10, 1996), summary affirmance granted, No. 97-5044 (D.C. Cir. June 5, 1997)). In addition, courts have also determined that this exemption covers investigations into potential threats to national security (see, e.g., Strang v. U.S. Arms Control & Disarmament Agency, 864 F.2d 859, 862-63 n.2 (D.C. Cir. 1989) ("this case involves not a job applicant undergoing a routine check of his background and his ability to perform the job, but an existing agency employee investigated for violating national security regulations.")

Routine background investigation files are generally not exempt under the (k)(2) exemption of the Privacy Act, but in some limited cases portions of them may be exempt under (k)(2) because they also include information that would be the subject of a law enforcement investigation under the scope of the exemption (see, e.g., Cohen v. FBI, No. 93-1701, slip op. at 4-6 (D.D.C. Oct. 3, 1995) (finding that particular information within a background investigation file qualified as "law enforcement" information "withheld out of a legitimate concern for national security," and that "'[s]o long as the investigation was "realistically based on a legitimate concern that federal laws have been or may be violated or that national security may be breached" the records may be considered law enforcement records'" (quoting Vymetalik v. FBI, 785 F.2d 1090, 1098 (D.C. Cir. 1986), in turn quoting Pratt v. Webster, 673 F.2d 408, 421 (D.C. Cir. 1982))).

NARA maintains a centralized hub for insider threat analysis to 1) manually and electronically gather, integrate, review, assess, and respond to information derived from internal

and external sources, and 2) identify potential insider threat concerns and conduct an appropriate inquiry to resolve the concern. Section 811 of the Intelligence Authorization Act for FY 1995; executive orders 13587, 13526, 12333, and 10450; Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, November 21, 2012; Presidential Memorandum, Early Detection of Espionage and Other Intelligence Activities through Identification and Referral of Anomalies, August 23, 1996; and Presidential Decision Directive/NSC-12, Security Awareness and Reporting of Foreign Contacts, August 5, 1993, authorize these insider threat assessment and investigation activities. As a result, the records in this system of records qualify as investigative records compiled for law enforcement purposes under the meaning of the Privacy Act's (k)(2) exemption. NARA is revising its regulations to exempt this information from disclosure under the Privacy Act so that it can prevent these investigations from being impeded or damaged by releasing the information.

Regulatory analysis

Review under Executive Orders 12866 and 13563

Executive Order 12866, Regulatory Planning and Review, 58 FR 51735 (September 30, 1993), and Executive Order 13563, Improving Regulation and Regulation Review, 76 FR 23821 (January 18, 2011), direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). This rule is not "significant" under section 3(f) of Executive Order 12866 because will not create an economic or budgetary impact, create an inconsistency or interfere with other agencies, and does not raise novel issues; it exempts certain records from

certain provisions of the Privacy Act in accord with established criteria. The Office of Management and Budget (OMB) has reviewed this regulation.

Review under the Regulatory Flexibility Act (5 U.S.C. 601, *et seq.*)

This review requires an agency to prepare an initial regulatory flexibility analysis and publish it when the agency publishes the proposed rule. This requirement does not apply if the agency certifies that the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities (5 U.S.C. 603). NARA certifies, after review and analysis, that this rule will not have a significant adverse economic impact on small entities because it does not create an economic impact and does not affect small entities; it exempts certain records from certain provisions of the Privacy Act.

Review under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501*et seq.*)

This rule does not contain any information collection requirements subject to the Paperwork Reduction Act.

Review under Executive Order 13132, Federalism, 64 FR 43255 (August 4, 1999)

Review under Executive Order 13132 requires that agencies review regulations for federalism effects on the institutional interest of states and local governments, and, if the effects are sufficiently substantial, prepare a Federal assessment to assist senior policy makers. This rule will not have any direct effects on State and local governments within the meaning of the Executive Order. Therefore, the regulation requires no federalism assessment.

List of Subjects in 36 CFR Part 1202

Privacy.

For the reasons stated in the preamble, NARA proposes to amend 36 CFR part 1202 as follows:

PART 1202---REGULATIONS IMPLEMENTING THE PRIVACY ACT OF 1974

1. The authority citation for part 1202 remains as follows:

Authority: 5 U.S.C. 552(a); 44 U.S.C. 2104(a).

§1202.92 [Amended]

2. Revise § 1202.92 to read as follows:

§ 1202.92 What NARA systems of records are exempt from release under the Law Enforcement Exemption of the Privacy Act?

(a) The Investigative Files of the Inspector General (NARA-23) and the Insider Threat Program Records (NARA-45) systems of records are eligible for exemption under 5 U.S.C. 552a(k)(2) because these record systems contain investigatory material of actual, potential, or alleged criminal, civil, or administrative violations, compiled for law enforcement purposes other than within the scope of subsection (j)(2) of 5 USC 552a. If you are denied any right, privilege, or benefit to which you would otherwise be entitled by Federal law, or for which you would otherwise be eligible, as a result of the record, NARA will make the record available to you, except for any information in the record that would disclose the identity of a confidential source as described in 5 U.S.C. 552a(k)(2).

(b) The systems described in paragraph (a) of this section are exempt from 5 U.S.C. 552a (c)(3), (d), (e)(1) and (e)(4), (G) and (H), and (f). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) of 5 U.S.C. 552a because releasing disclosure accounting could alert the subject of an investigation about the alleged violations, about the existence of the

investigation, and about the fact that they are being investigated by the Office of Inspector General (OIG), the Insider Threat Office, or another agency. Releasing these records could provide significant information concerning the nature of the investigation and result in tampering with or destroying evidence, influencing witnesses, endangering individuals involved, and other activities that could impede or compromise the investigation.

(2) From the access and amendment provisions of subsection (d) of 5 U.S.C. 552a because access to the information contained in these systems of records could inform the subject of an investigation about an actual or potential criminal, civil, or administrative violation; about the existence of that investigation; about the nature and scope of the information and evidence obtained on the person's activities; about the identity of confidential sources, witnesses, and law enforcement personnel; and about information that may enable the person to avoid being detected or apprehended. These factors present a serious impediment to effective law enforcement when they prevent investigators from successfully completing the investigation, endanger the physical safety of confidential sources, witnesses, and law enforcement personnel, or lead to improperly influencing witnesses, destroying evidence, or fabricating testimony. In addition, granting access to such records could disclose security-sensitive or confidential business information or information that would constitute an unwarranted invasion of the personal privacy of third parties. Amending these records could allow the subject to avoid being detected or apprehended and interfere with ongoing investigations and law enforcement activities.

(3) From subsection (e)(1) of 5 U.S.C. 552a because applying this provision could impair investigations and interfere with the law enforcement responsibilities of the OIG, the Insider Threat Office, or another agency for the following reasons:

(i) It is not possible to detect relevance or need for specific information in the early stages of an investigation, case, or matter. After the investigators evaluate the information, they may establish its relevance and need.

(ii) During an investigation, the investigating office may obtain information about other actual or potential criminal, civil, or administrative violations, including those outside the scope of its jurisdiction. The office should retain this information, as it may help establish patterns of inappropriate activity, and can provide valuable leads for Federal and other law enforcement agencies.

(iii) When interviewing individuals or obtaining other forms of evidence during an investigation, the investigator may receive information that relates to matters incidental to the primary purpose of the investigation but which may also relate to matters under the investigative jurisdiction of another office or agency. The investigator cannot readily segregate such information.

(4) From subsection (e)(4)(G) and (H) of 5 U.S.C. 552a because these systems are exempt from the access and amendment provisions of subsection (d), pursuant to subsection (k)(2) of the Privacy Act.

(5) From subsection (f) of 5 U.S.C. 552a because these systems are exempt from the access and amendment provisions of subsection (d) of 5 U.S.C. 552a, pursuant to subsection (k)(2) of the Privacy Act.

Dated: May 29, 2016

DAVID S. FERRIERO

Archivist of the United States.

[FR Doc. 2016-13599 Filed: 6/7/2016 8:45 am; Publication Date: 6/8/2016]