Billing Code: 7515-01U

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

NARA-2016-033

Privacy Act of 1974, as Amended; System of Records Notice

AGENCY: National Archives and Records Administration (NARA).

ACTION: Privacy Act system of records notice (SORN) of a new system, NARA 45.

SUMMARY: The National Archives and Records Administration (NARA) proposes to add 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"). In this notice, NARA publishes NARA 45, Insider Threat Program records. In addition, NARA is updating Appendix B to add the SORN's system manager to the list of system managers and their addresses.

DATES: This new system of records, NARA 45, and Appendix B update will become effective [INSERT DATE 40 DAYS FROM PUBLICATION] without further notice unless we receive comments by [INSERT DATE 30 DAYS FROM PUBLICATION] that cause us to revise it. NARA will publish a new notice if we must delay the effective date to review comments or make changes.

ADDRESSES: You may submit comments, identified by "SORN NARA 45," by one of the following methods:

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

- Email: Regulation_comments@nara.gov. Include SORN NARA 45 in the subject line of the message.
- Mail (for paper, disk, or CD-ROM submissions. Include SORN NARA 45 on the submission): Regulations Comment Desk, Strategy and Performance Division (SP); Suite 4100; National and Archives 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 SORN NARA 45. We may publish any comments we receive without changes, including any personal information you include.

FOR FURTHER INFORMATION CONTACT: For more information related to the SORN process, contact Kimberly Keravuori, External Policy Program Manager, by email at regulation_comments@nara.gov, or by telephone at 301-837-3151. For information on the records, contact Neil Carmichael, Insider Threat Program Director, by mail at National Archives and Records Administration; 8601 Adelphi Road; College Park, MD 20740-6001, or by telephone at 301-837-3169.

SUPPLEMENTARY INFORMATION: The notice for this system of records states the record system's name and location, authority for and manner of operation, categories of individuals it covers, types of records it contains, sources of information in the records, and the "routine uses" for which the agency may use the information. Appendix B includes the business

address of the NARA official you may contact to find out how you may access and correct records pertaining to yourself.

The Privacy Act provides certain safeguards for an individual against an invasion of personal privacy. It requires Federal agencies that disseminate any record of personally identifiable information to do so in a manner that assures the action is for a necessary and lawful purpose, the information is current and accurate for its intended use, and adequate safeguards are provided to prevent misuse of such information. NARA intends to follow these principles when transferring information to another agency or individual as a "routine use," including assuring that the information is relevant for the purposes for which it is transferred.

In addition, the Privacy Act allows agencies to exempt from release certain information compiled for law enforcement purposes. By a separate, concurrent rulemaking action, NARA is exempting this system of records for that purpose. See the final rule published elsewhere in this issue of the Federal Register.

Dated: May 29, 2016

David S. Ferriero

Archivist of the United States.

NARA 45

SYSTEM NAME:

Insider Threat Program Records

SYSTEM LOCATION:

The Office of the Chief Operating Officer at the National Archives in College Park maintains insider threat program records.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals covered by this system include future, current, and former NARA employees, NARA contractors, employees and contractors of other Federal agencies who have access to classified information within NARA facilities, Presidential representatives at Presidential libraries, and members of the Public Interest Declassification Board. Other covered individuals include officials or employees of Federal, state, tribal, territorial, and local law enforcement organizations; complainants, informants, suspects, and witnesses; people with access to NARA facilities and infrastructure; members of the general public, including individuals and groups of individuals involved with insider threat matters, complaints, or incidents involving classified systems or classified information; individuals being investigated as potential insider threats; pose a threat to NARA operations, data, personnel, facilities, and systems; and foreign visitors or foreign contacts.

CATEGORIES OF RECORDS IN THE SYSTEM:

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.

NARA monitors user activity on all information technology networks or stand-alone systems, including use by both cleared and un-cleared employees. The Insider Threat Program may use this monitoring information to detect activity that might indicate insider threat behavior. The system includes records from this activity, including monitoring logs and insider threat analyses. The Insider Threat Program may also make use of records from other NARA Privacy Act systems of records. When this occurs, records from those other systems will also become part of this system of records. The other systems of records involved include: NARA 7: Freedom of Information Act (FOIA) and Mandatory Review of Classified Documents Request Files; NARA 8: Restricted and Classified Records Access Authorization Files, NARA 11: Credentials and Passes; NARA 12: Emergency Notification Files and Employee Contact Information; NARA 14: Payroll, Attendance, Leave, Retirement, Benefits, and Electronic Reporting System Records; NARA 17: Grievance Records; NARA 18: General Law Files; NARA 19: Workers' Compensation Case Files; NARA 22: Employee-Related Files; NARA 23: Office of Inspector General Investigative Case Files; NARA 24: Personnel Security Files; NARA 26: Volunteer and Unpaid Student Intern Files; NARA 27: Contracting Officer and Contracting Officer's Representative (COR) Designation Files; NARA 28: Tort and Employee Claim Files; NARA 30: Garnishment Files; NARA 32: Alternate Dispute Resolution Files; NARA 34: Agency Ethics Program Files; NARA 35: Case Management and Reporting System (CMRS); and NARA 43: Internal Collaboration Network (ICN).

In addition, this system of records may contain information from NARA offices, programs, databases, records, or sources, including incident reports, investigatory records, personnel security records, facility access records, network security records, security violations, travel records, foreign visitor records, foreign contact reports, financial disclosure reports, personnel records, medical records, information on complainants, informants, suspects, and witnesses, and records involving potential insider threats or activities.

All the records in this system of records may contain the following information on an individual: name, social security number, date of birth, place of birth, security clearance, home address, work address, personal and official phone numbers, personal and official email addresses, other contact information, driver license number, vehicle identification number, license plate number, ethnicity and race, tribal identification number or other tribal enrollment data, work history, educational history, arrest reports, references to illegal drug involvement, mental health records including counseling related to use of alcohol or drugs, civil court action records, subversive activity information, outside affiliations, information on family members, dependents, relatives, and other personal associations, passport number, gender, fingerprints, hair and eye color, biometric data, and any other individual physical or distinguishing attributes.

Investigation records and incident reports may include additional information on an individual, such as: photos, video, sketches, medical reports, network use records, identification badge data, facility and access control records, email, and text messages.

The records may also include information concerning potential insider threat activity, counterintelligence complaints, investigative referrals, results of incident investigations, case

numbers, forms, nondisclosure agreements, consent forms, documents, reports, and correspondence received, generated, or maintained in the course of managing insider threat activities and conducting investigations related to potential insider threats.

Finally, this system contains records of inquiries the hub creates in the course of managing the Insider Threat Program. An inquiry record is akin to a case file on a possible insider threat, and may contain any of the information described above, in addition to investigatory records such as interview notes, analysis of the potential threat, voluntary statements to investigators, and similar documents.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

44 U.S.C. 2104(a), as amended;

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.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

NARA maintains insider threat program records on people to: manage insider threat matters; facilitate insider threat inquiries, investigations, and activities associated with counterintelligence complaints, inquiries, and investigations; identify potential threats; track referrals of potential insider threats to internal and external partners; provide statistical reports; and meet other insider threat reporting requirements.

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside NARA as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

(1) To the Executive Office of the President in response to an inquiry from that office made at the request of the subject of a record or a third party on that person's behalf, or for a purpose compatible to those for which the records are collected or maintained, to the extent the records have not been exempted from disclosure pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

(2) To an official of another Federal agency to provide information the agency needs to perform official duties related to reconciling or reconstructing data files or to enable that agency to respond to an inquiry by the individual to whom the record pertains.

(3) To state, local, and tribal governments to provide information in response to a court order or litigation discovery requests, when disclosure is compatible with the purpose for which the records were compiled.

(4) To other appropriate agencies, entities, and people when:

(a) NARA suspects or confirms that the security or confidentiality of information in the system of records has been compromised; and

(b) NARA has determined that, as a result of the suspected or confirmed compromise, there is a risk of harm to economic or property interest, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by NARA or another agency or entity) that rely upon the compromised information; and

(c) NARA discloses the information to such agencies, entities, and people who are reasonably necessary to assist in connection with NARA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

(5) To the Office of Management and Budget during legislative coordination and clearance as mandated by OMB Circular A-19.

(6) To the Department of the Treasury to recover debts owed to the United States.

(7) To the Department of Justice, the Federal Bureau of Investigation, the Department of Homeland Security, and other Federal, state and local law enforcement agencies to refer potential insider threats to them and exchange information on insider threat activity.

(8) To any criminal, civil, or regulatory authority (whether Federal, state, territorial, local, or tribal) to provide background search information on individuals for legally authorized purposes, including but not limited to background checks on individuals residing in a home with a minor or individuals seeking employment opportunities requiring background checks.

Routine uses A, B, C, D, E, F, G, and H listed in Appendix A also apply to this system.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Paper and electronic records

RETRIEVABILITY:

Staff may retrieve information in these records by the employee's name, by search, or by any available field or metadata element recorded in the system.

SAFEGUARDS:

During normal hours of operation, NARA maintains paper records in areas accessible to authorized NARA personnel. Staff access electronic records via password-protected workstations located in attended offices or through a secure remote access network. After hours, buildings have security guards or secured doors, and electronic surveillance equipment monitors all entrances.

RETENTION AND DISPOSAL:

NARA insider threat program records are unscheduled records; NARA therefore retains them until the Archivist of the United States approves dispositions for them.

SYSTEM MANAGER AND ADDRESS:

The system manager for the insider threat program records is the Chief Operating Officer. The business addresses for system managers are listed in Appendix B.

NOTIFICATION PROCEDURE:

People inquiring about their records should notify the NARA Privacy Act Officer at the address listed in Appendix B. However, NARA proposes to exempt portions of this system from the notification procedures of the Privacy Act, pursuant to section and (k)(2).

RECORDS ACCESS PROCEDURES:

People who wish to access their records should submit a request in writing to the NARA Privacy Act Officer at the address listed in Appendix B. However, NARA proposes to exempt portions of this system from the access procedures of the Privacy Act, pursuant to section and (k)(2).

CONTESTING RECORDS PROCEDURES:

NARA's rules for contesting the contents of your records and appealing initial determinations are in 36 CFR Part 1202. However, NARA proposes to exempt portions of this system from the amendment procedures of the Privacy Act, pursuant to section and (k)(2).

RECORD SOURCE CATEGORIES:

NARA may obtain information in the system from NARA office and program officials, employees, contractors, and other individuals associated with or representing NARA; officials from other Federal, tribal, territorial, state, and local government organizations; relevant NARA records, databases, and files, including personnel security files, facility access records, security incident or violation files, network security records, investigatory records, visitor records, travel records, foreign visitor or contact reports, and financial disclosure reports; and complainants, informants, suspects, and witnesses.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

This system contains classified and unclassified intelligence and law enforcement investigatory records related to counterintelligence and insider threat activities that are **e**xempt from certain provisions of the Privacy Act; specifically, 5 U.S.C. 552a (k)(2). Pursuant to subsection (k)(2), NARA exempts portions of this system from the following subsections of the Privacy Act: (c)(3), (d), (e)(1) and (e)(4)(G) and (H), and (f). In accordance with 5 U.S.C. 553(b), (c), and (e), NARA has promulgated Regulations Implementing the Privacy Act of 1974, at 36 CFR 1202, that establish this exemption (see 36 CFR 1202.92). NARA is concurrently revising its regulation to add this system of records, as published elsewhere in this issue of the Federal Register.

APPENDIX B

Records inquiries and requests:

To inquire about your records or to gain access to your records, you should submit your request in writing to: NARA Privacy Act Officer; Office of the General Counsel (NGC); National Archives and Records Administration; 8601 Adelphi Road, Room 3110; College Park, MD 20740-6001.

System managers:

If the system manager is the **Chief Human Capital Officer**, the business address is: Office of Human Capital; National Archives and Records Administration; 8601 Adelphi Road, Room 1200; College Park, MD 20740-6001.

If the system manager is the **Chief Information Officer**, the business address is: Office of Information Services; National Archives and Records Administration; 8601 Adelphi Road, Room 4400; College Park, MD 20740-6001.

If the system manager is the **Chief Innovation Officer**, the business address is: Office of Innovation; National Archives and Records Administration; 8601 Adelphi Road, Room 3200; College Park, MD 20740-6001.

If the system manager is the **Chief Operating Officer**, the business address is: Office of the Chief Operating Officer; National Archives and Records Administration; 8601 Adelphi Road, Room 4200; College Park, MD 20740-6001.

If the system manager is the **Chief Records Officer**, the business address is: Office of the Chief Records Officer; National Archives and Records Administration; 8601 Adelphi Road, Room 2100; College Park, MD 20740.

If the system manager is the **Chief Strategy and Communications Officer**, the business address is: Office of Strategy and Communications; National Archives and Records Administration; 8601 Adelphi Road, Room 4100; College Park, MD 20740-6001.

If the system manager is the **Designated Agency Ethics Official**, the business address is: Office of the General Counsel; National Archives and Records Administration; 8601 Adelphi Road, Room 3110; College Park, MD 20740-6001.

If the system manager is the **Director, National Personnel Records Center**, the business address is: National Personnel Records Center, 1 Archives Drive, St. Louis, MO 63138.

If the system manager is the **director of an individual Presidential library**, the business address is the relevant Presidential library:

George H.W. Bush Library, 1000 George Bush Drive West, College Station, TX 77845

George W. Bush Library, 2943 SMU Boulevard, Dallas, TX 75205

Jimmy Carter Library, 441 Freedom Parkway, Atlanta, GA 30307-1498

William J. Clinton Library, 1200 President Clinton Avenue, Little Rock, AR 72201

Dwight D. Eisenhower Library, 200 SE 4th Street, Abilene, KS 67410-2900

Gerald R. Ford Library, 1000 Beal Avenue, Ann Arbor, MI 48109-2114

Herbert Hoover Library, 210 Parkside Drive, P.O. Box 488, West Branch, IA 52358-0488

Lyndon B. Johnson Library, 2313 Red River Street, Austin, TX 78705-5702

John F. Kennedy Library, Columbia Point, Boston, MA 02125-3398

Richard Nixon Library, 1800 Yorba Linda Boulevard, Yorba Linda, CA 92886

Ronald Reagan Library, 40 Presidential Drive, Simi Valley, CA 93065-0600

Franklin D. Roosevelt Library, 4079 Albany Post Road, Hyde Park, NY 12538-1999

Harry S. Truman Library, 500 West U.S. Highway 24, Independence, MO 64050-1798

If the system manager is the **Director, Office of Equal Employment Opportunity**, the business address is: Office of Equal Employment Opportunity; National Archives and Records Administration; 8601 Adelphi Road, Room 3310; College Park, MD 20740-6001.

If the system manager is the **Director of the Center for Legislative Archives**, the business address is: The Center for Legislative Archives; National Archives and Records Administration; 700 Pennsylvania Ave., NW; Washington, DC 20408-0001.

If the system manager is the **Director of the Federal Register**, the business address is: Office of the Federal Register; National Archives and Records Administration; 800 North Capitol Street, NW; Washington, DC 20002.

If the system manager is the **Director of the Office of Presidential Libraries**, the business address is the Office of Presidential Libraries; National Archives and Records Administration; 8601 Adelphi Road, Room 2200; College Park, MD 20740-6001.

If the system manager is the **Director of the Presidential Materials Division**, the business address is: Presidential Materials Division; National Archives and Records Administration; 700 Pennsylvania Ave., NW, Room 104; Washington, DC 20408-0001.

If the system manager is the **Director of the Washington National Records Center**, the records are located at the following address: Washington National Records Center; National Archives and Records Administration; 4205 Suitland Road; Suitland, MD 20746-8001.

If the system manager is the **Executive Director of the National Historical Publications and Records Commission**, the business address is: National Historical Publications and Records Commission; National Archives and Records Administration; 700 Pennsylvania Avenue, NW, Room 114; Washington, DC 20408-0001.

If the system manager is the **Executive for Agency Services**, the business address is: Office of Agency Services; National Archives and Records Administration; 8601 Adelphi Road, Room 3600; College Park, MD 20740-6001.

If the system manager is the **Executive for Business Support Services**, the business address is: Office of Business Support Services; National Archives and Records Administration; 8601 Adelphi Road, Room 5100; College Park, MD 20740-6001.

If the system manager is the **Executive for Information Services**, the business address is: Office of Information Services; National Archives and Records Administration; 8601 Adelphi Road, Room 4400; College Park, MD 20740-6001.

If the system manager is the **Executive for Legislative Archives, Presidential Libraries, and Museum Services**, the business address is the Office of Legislative Archives, Presidential Libraries, and Museum Services; National Archives and Records Administration; 700 Pennsylvania Avenue, NW, Room 104; Washington, DC 20408-0001.

If the system manager is the **Executive for Research Services**, the business address is: Office of Research Services; National Archives and Records Administration; 8601 Adelphi Road, Room 3400; College Park, MD 20740-6001.

If the system manager is the **General Counsel**, the business address is: Office of the General Counsel; National Archives and Records Administration; 8601 Adelphi Road, Room 3110; College Park, MD 20740-6001.

If the system manager is the **Inspector General**, the business address is: Office of the Inspector General; National Archives and Records Administration; 8601 Adelphi Road, Room 1300; College Park, MD 20740-6001.

[FR Doc. 2016-13600 Filed: 6/7/2016 8:45 am; Publication Date: 6/8/2016]