DEPAR

Privacy Act of 1974; System of Records

AGENCY: Human Resources and Administration/Operations, Security, and Preparedness, Department of Veterans Affairs (VA).

ACTION: Notice of a new system of records.

SUMMARY: Pursuant to the Privacy Act of 1974, notice is hereby given that the Department of Veterans Affairs (VA) proposes to establish a new system of records, entitled, “Insider Threat Program-VA” (196VA007). This System of Records allows VA to establish capabilities to detect, deter, and mitigate insider threats. VA will use the System of Records to facilitate management of insider threat inquiries; identify potential threats to VA resources and information assets; manage referrals of potential insider threats to and from internal and external partners; provide authorized assistance to lawful administrative, civil, counterintelligence, and criminal investigations; and provide statistical reports and meet other insider threat reporting requirements.

DATES: Comments on this new system of records must be received no later than 30 days after date of publication in the *Federal Register*. If no public comment is received during the period allowed for comment or unless otherwise published in the F*ederal Register* by VA, the new system of records will become effective a minimum of 30 days after date of publication in the *Federal Register*. If VA receives public comments, VA shall review the comments to determine whether any changes to the notice are necessary.

FOR FURTHER INFORMATION CONTACT: Terry Clyburn, Director Operations and National Security Services, Department of Veterans Affairs 810 Vermont Avenue, NW, Washington, DC 20420; terry.clyburn@va.gov; 202-461-5563.

SUPPLEMENTARY INFORMATION: Executive Order (E.O.) 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and

Safeguarding of Classified Information, (October 7, 2011), requires Federal agencies to establish an insider threat detection and prevention program to ensure the security of classified networks and the responsible sharing and safeguarding of classified information with appropriate protections for privacy and civil liberties. Once E.O. 13587 was issued, VA initiated an Insider Threat Program (ITP) to meet these requirements. Insider threats can include any of the following: attempted or actual espionage, subversion, sabotage, terrorism, or extremist activities directed against the Department and its personnel, facilities, information resources, and activities; unauthorized use of or intrusion into automated information systems; unauthorized disclosure of classified, controlled unclassified, sensitive, or proprietary information to technology; indicators of potential insider threats or other incidents that may indicate activities of an insider threat; and other threats to the Department, such as indicators of potential for workplace violence or misconduct. The records that the ITP will compile in support of the Program may originate from any VA component, office, program, record, or source, and may include records pertaining to information security, personnel security, or systems security.

Signing Authority

The Senior Agency Official for Privacy, or designee, approved this document and authorized the undersigned to sign and submit the document to the Office of the Federal Register for publication electronically as an official document of the Department of Veterans Affairs. Kurt D. DelBene, Assistant Secretary for Information and Technology and Chief Information Officer, approved this document on January 6, 2023 for publication.

Dated: February 22, 2023.

Amy L. Rose,

Program Analyst,

VA Privacy Service,

Office of Information Security,

Office of Information and Technology,

Department of Veterans Affairs.

SYSTEM NAME AND NUMBER: Insider Threat Program-VA (196VA007).

SECURITY CLASSIFICATION: Unclassified and classified.

SYSTEM LOCATION: Systems of records are generally maintained on information systems owned, operated by, or operated on behalf of the Department. Records in this system are maintained at 810 Vermont Ave NW, Washington, DC, 20420.

SYSTEM MANAGER(S): Program Manager, Insider Threat Analytic Team (202-461-5900), Office of Operations, Security, and Preparedness, Department of Veterans Affairs, 810 Vermont Ave, NW, Washington, DC 20420, James Babin, james.babin@va.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (Oct. 7, 2011); E.O. 13526, Classified National Security Information (December 29, 2009); E.O. 12968, Access to Classified Information (August 4, 1995); Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (November 21, 2012); VA Directive 0327, Insider Threat Policy (February 5, 2015).

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to detect, deter, and mitigate insider threats. VA will use the system to facilitate management of insider threat inquiries; identify and track potential insider threats to VA; manage referrals of potential insider threats to and from internal and external partners; provide authorized assistance to lawful administrative, civil, counterintelligence, and criminal investigations; and generate statistical reports and meet other insider threat reporting requirements.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: These records include information on Veterans Affairs “insiders” as defined above, which include present and former VA employees, contractors, detailees, assignees, interns, visitors, and guests. In addition, persons who report concerns, witnesses, relatives, and individuals with other

relevant personal associations with the insider are covered by the system of records notice.

CATEGORIES OF RECORDS IN THE SYSTEM: The records may include:

Information potentially relevant to resolving possible insider threats and lawful DHS security investigations, including authorized physical, personnel, and communications security investigations, and information systems security analysis and reporting. Such information may include:

- Individual's name and alias(es);
- Date and place of birth;
- Social Security number;
- Address;
- Open source information, including publicly available social media information;
- Personal and official email addresses;
- Citizenship;
- Personal and official phone numbers;
- Driver license number(s);
- Vehicle Identification Number(s);
- License plate number(s);
- Ethnicity and race;
- Current Employment and Performance Information;
- Work history;
- Education history;
- Contract information;
- Information on family members, dependents, relatives and other personal associations;
- Passport number(s); DHS-held Travel records;

- Gender;
- Hair and eye color;
- Biometric data;
- Other physical or distinguishing attributes of an individual;
- Medical information;
- Access control pass, credential number, or other identifying number(s);
- Media obtained through authorized procedures, such as CCTV footage; and
- Any other information provided to obtain access to DHS facilities or information systems.
- Records relating to the management and operation of the DHS physical, personnel, and communications security programs, including:
- Completed standard form questionnaires issued by the Office of Personnel Management;
- Background investigative reports and supporting documentation, including criminal background, medical, and financial data;
- Current and former clearance status(s);
- Other information related to an individual's eligibility for access to classified information;
- Criminal history records;
- Polygraph examination results;
- Logs of computer activities on all DHS IT systems or any IT systems accessed by DHS personnel;
- Nondisclosure agreements;
- Document control registries;
- Courier authorization requests;
- Derivative classification unique identifiers;

- Requests for access to sensitive compartmented information (SCI);
- Records reflecting personal and official foreign travel;
- Facility access records;
- Records of contacts with foreign persons; and
- Briefing/debriefing statements for special programs, sensitive positions, and other related information and documents required in connection with personnel security clearance determinations.
- Reports of investigations or inquiries regarding security violations or misconduct, including:
- Individuals' statements or affidavits and correspondence;
- Incident reports;
- Drug test results;
- Investigative records of a criminal, civil, or administrative nature;
- Letters, emails, memoranda, and reports;
- Exhibits, evidence, statements, and affidavits;
- Inquiries relating to suspected security violations;
- Recommended remedial actions for possible security violations; and
- Personnel files containing information about misconduct and adverse actions.
- Any information related to the management and operation of the DHS ITP, including:
- Documentation pertaining to fact-finding or analytical efforts by ITP personnel to identify insider threats to DHS resources, personnel, property, facilities, or information;
- Records of information technology events and other information that could reveal potential insider threat activities;
- Intelligence reports and database query results relating to individuals covered by this system;

- Information obtained from the Intelligence Community, law enforcement partners, and from other agencies or organizations about individuals and/or organizations known or reasonably suspected of being engaged in conduct constituting, preparing for, aiding, or relating to an insider threat;
- Information provided by subjects and individual members of the public; and
- Information provided by individuals who report known or suspected insider threats.

RECORD SOURCE CATEGORIES: Records are obtained from (1) software that monitors VA users' activity on U.S. Government computer networks; (2) information supplied by individuals to the Department or by the individual's employer; (3) information provided to the Department to gain access to VA facilities, information, equipment, networks, or systems; (4) publicly available information obtained from open source platforms, including publicly available social media; (5) any departmental records for which the Insider Threat Program (ITP) has been given authorized access; and (6) any federal, state, local government, or private sector records for which the ITP has been given authorized access. The Insider Threat Analytic Response Team (ITART) also receives tips and leads by other means, such as email or telephone. The ITART may receive a tip from any party, including members of the public.

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

1. Congress: To a Member of Congress or staff acting upon the Member’s behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

2. Data Breach Response and Remediation, for VA: To appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that there has been a breach of the system of records,· (2) VA has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, VA (including its information

systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with VA's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

3. Data Breach Response and Remediation, for Another Federal Agency: To another Federal agency or Federal entity, when VA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

4. Law Enforcement: To a Federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law, provided that the disclosure is limited to information that, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature. The disclosure of the names and addresses of veterans and their dependents from VA records under this routine use must also comply with the provisions of 38 U.S.C. 5701.

5. DoJ, Litigation, Administrative Proceeding: To the Department of Justice (DoJ), or in a proceeding before a court, adjudicative body, or other administrative body before which VA is authorized to appear, when:

(a) VA or any component thereof;

(b) Any VA employee in his or her official capacity;

(c) Any VA employee in his or her individual capacity where DoJ has agreed to represent the employee; or

(d) The United States, where VA determines that litigation is likely to affect the agency or any of its components,

is a party to such proceedings or has an interest in such proceedings, and VA determines that use of such records is relevant and necessary to the proceedings.

6. Contractors: To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for VA, when reasonably necessary to accomplish an agency function related to the records.

7. OPM: To the Office of Personnel Management (OPM) in connection with the application or effect of civil service laws, rules, regulations, or OPM guidelines in particular situations.

8. EEOC: To the Equal Employment Opportunity Commission (EEOC) in connection with investigations of alleged or possible discriminatory practices, examination of Federal affirmative employment programs, or other functions of the Commission as authorized by law.

9. FLRA: To the Federal Labor Relations Authority (FLRA) in connection with the investigation and resolution of allegations of unfair labor practices, the resolution of exceptions to arbitration awards when a question of material fact is raised, matters before the Federal Service Impasses Panel, and the investigation of representation petitions and the conduct or supervision of representation elections.

10. MSPB: To the Merit Systems Protection Board (MSPB) in connection with appeals, special studies of the civil service and other merit systems, review of rules and regulations, investigation of alleged or possible prohibited personnel practices, and such other functions promulgated in 5 U.S.C. 1205 and 1206, or as authorized by law.

11. NARA: To the National Archives and Records Administration (NARA) in records management inspections conducted under 44 U.S.C. 2904 and 2906, or other functions

authorized by laws and policies governing NARA operations and VA records management responsibilities.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records are retrieved by first and last name, Social Security number, date of birth, phone number, other unique individual identifiers, and other types of information by key word search.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, VHA RCS 10-1, Item Numbers 5252.21-5252.24.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: VA ITP safeguards records in this system according to applicable rules and policies, including all applicable VA automated systems security and access policies. VA has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES: Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing as indicated above. A request for access to records must contain the requester’s full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort. Please note: some records in this system are exempt from record access and amendment provisions of 5 U.S.C. 552a(k).

CONTESTING RECORD PROCEDURES: Individuals seeking to contest or amend records in this system pertaining to them should contact the system manager in writing as indicated above. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record. Please note: some records in this system are exempt from record access and amendment provisions of 5 U.S.C. 552a(k).

NOTIFICATION PROCEDURES: Generalized notice is provided by the publication of this notice. For specific notice, see Record Access Procedure, above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: The Secretary of Veterans Affairs, pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5), has exempted law enforcement investigatory material and classified intelligence information in this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). When this system receives a record from another system exempted under 5 U.S.C. 552a, VA will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

HISTORY: None.

[FR Doc. 2023-03938 Filed: 2/24/2023 8:45 am; Publication Date: 2/27/2023]