This document is scheduled to be published in the Federal Register on 01/25/2021 and available online at **federalregister.gov/d/2021-01528**, and on **govinfo.gov**

**DEPARTMI**

**Privacy Act of 1974; System of Records**

**AGENCY:** Department of Veterans Affairs (VA).

**ACTION:** Notice of amendment to an existing System of Records.

**SUMMARY:** As required by the Privacy Act of 1974, notice is hereby given that the Department of Veterans Affairs is amending the system of records currently entitled "Non-Health Data Analyses and Projections for VA Policy and Planning-VA (149VA008A)" as set forth in the Federal Register. VA is amending this system notice serves to reflect amendments to the amendments to the Routine Uses of Records Maintained in the System, Safeguards, Retention and Disposal, and System Manager and Address as well as Notification Procedure. VA is republishing the system notice in its entirety.

**DATES:** This amended system of record will be effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN FEDERAL REGISTER]**.

**ADDRESSES:** Written comments may be submitted by: mail or hand-delivery to the Director, Regulations Management (02REG), Department of Veterans Affairs, 810 Vermont Ave., NW, Room 1068, Washington, DC 20420; fax to (202) 273-9026 or email to http://www.Regulations.gov. All copies of comments received will be available for public inspection in the Office of Regulation Policy and Management, Room 1063B, between the hours of 8:00 a.m. and 4:30 p.m., Monday through Friday (except holidays). Please call (202) 461-4902 (This is not a toll-free number) for an appointment.

**FOR FURTHER INFORMATION CONTACT:** Office of Enterprise Integration (OEI), Ryan J. Stiegman, Privacy Officer, U.S. Department of Veterans Affairs, 810 Vermont Ave., NW., Washington, DC 20420; telephone (202) 461-5800.

**SUPPLEMENTARY INFORMATION:**

Non-Health Data Analyses and Projections for VA Policy and Planning-VA (149VA008A) have been amended to reflect new organizational names, new mail addresses, and updated point of contact information. Additionally, information technology guidance regarding storage and transmission has been updated. Also, Veteran Affairs has made minor edits to the System Notice to standardize language. Finally, an obsolete web address has been updated to a more complete description of the duties of the Office of Enterprise.

The Record Source Categories has been amended to identify the organizational name to the Office of Enterprise Integration that replaces the Office of Policy and Planning.

The Storage section has been amended to identify the organizational name to the Office of Enterprise Integration. Directive 6513 *Secure External Connections* has been added to clarify VA policy guidance. Finally, the Storage Section has been amended to reflect a change from “VA’s Austin Automation Center” to “VA’s Austin Information Technology Center” location

The Policies and Practices for Retrievability of Records have been amended to identify the organizational name to the Office of Enterprise Integration.

The Policies and Practices for retention and disposal have been amended to identify the organizational name to the Office of Enterprise Integration.

The Physical, Procedural and Administrative Safeguard section has been amended to clarify that a panel of staff for data requests is fulfilled in a data review process. This section has also changed concurrence authority to the Executive Director level from the Assistant Secretary level. Finally, the Office of Policy and Planning has been replaced with the Office of Enterprise Integration.

The System Manager organizational title has been changed from the Assistant Secretary to the Executive Director (008B). The System Manager address has been

amended from the Office of Policy and Planning to the successor organization of the Office of Enterprise Integration.

The Record Access section has been reformatted to VA standard and now includes two listed contacts for Veterans.

The Report of Intent to Amend a System of Records Notice and an advance copy of the system notice have been sent to the appropriate congressional committees and to the Director of the Office of Management and Budget (OMB) as required by 5 U.S.C. 552a(r) (Privacy Act) and guidelines issued by OMB (65 FR 77677), December 12, 2000.

**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. James P. Gfrerer, Assistant Secretary of Information and Technology and Chief Information Officer, approved this document on April 15, 2020 for publication.

Dated: January 19, 2021.

**Amy L. Rose,**

*Program Analyst,*

*VA Privacy Service,*

*Office of Information Security,*

*Office of Information and Technology,*

*Department of Veterans Affairs.*

**149VA008A**

**SYSTEM NAME: "**Non-Health Data Analyses and Projections for VA Policy and Planning—VA"

**SYSTEM LOCATION:**

Location for electronic records are placed in the Department of Veterans Affairs' (VA's) secured servers housed at VA's Austin Information Technology Center, 1615 Woodward St, Austin, TX 78772. Records necessary for a contractor to perform a VA-approved contract with VA are located at the respective contractor's facility.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:** Title 38, United States Code, Section 527

**PURPOSE(S):** Non-health-related qualitative, quantitative, and actuarial analyses and projections to support policy analyses and recommendations to improve VA services for Veterans and their families. Analysis and review of policy and long-term planning issues affecting Veterans programs support legislative, regulatory and policy recommendations, decisions and initiatives. These activities are conducted for the Secretary, VA administrations and staff offices, special programs and projects within the Department (e.g., special studies, advisory committees and task forces etc.), and entities external to VA, such as the Office of Management and Budget (OMB), and the United States (U.S.) Congress.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

1. Service members and Veterans who have applied for any non-health-related benefits under 38 U.S.C.

2. Veterans' spouse, surviving spouse, previous spouse, children, and parents who have applied for any non-health-related benefit under 38 U.S.C.

3. Beneficiaries of other Federal agencies or other governmental entities.

4. Individuals who have applied for any non-health-related benefits under 38 U.S.C., but who do not meet the requirements under 38 U.S.C. to receive such benefits.

**CATEGORIES OF RECORDS IN THE SYSTEM:** The records may include personal identifiers (e.g., social security numbers and military service numbers etc.), residential and professional contact data (e.g., address and telephone numbers etc.), population demographics (e.g., gender and zip codes etc.), military service-related data (e.g., branch of service and service dates etc.), financial-related data (e.g., amount of historic benefit payments etc.), interment and burial benefit information, claims processing codes and information (e.g., disability compensation and pension award codes etc.), and other VA and non-VA Federal information.

**RECORD SOURCE CATEGORIES:**

Information from the Office of Enterprise Integration is obtained from VA's benefits-related databases, DoD, Federal and State agencies, and other organizations whose data is necessary to accomplish the purpose for this system of records.

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

*NOTE:* To the extent that records contained in the system include individually-identifiable information protected by 38 U.S.C. 7332, that information cannot be disclosed under any of the following routine uses unless there is also specific disclosure authority in 38 U.S.C. 7332.

1. Breach investigation. Upon suspicion or confirmation of compromised data in its system of records, Office of Enterprise Integration (OEI) may disclose any system records to law enforcement and security entities, as necessary, for the investigations of any data security, identity theft, and fraud issues.

2. Congress. VA may disclose information from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

3. NARA & GSA. VA may disclose information from this system to the National Archives and Records Administration (NARA) and General Services Administration (GSA) in records management inspections conducted under title 44, U.S.C.

4. Litigation. Any information in this system may be disclosed to the Department of Justice (DOJ), including U.S. Attorneys, upon its official request in order for VA to respond to pleadings, interrogatories, orders or inquiries from DOJ, and to supply DOJ with information to enable DOJ to represent the U.S. Government in any phase of litigation or in any case or controversy involving VA.

5. Research. Any system records may be disclosed to a Federal agency for the conduct of research and data analysis to perform a statutory purpose of that Federal agency upon the prior written request of that agency, provided that there is legal authority under all applicable confidentiality statutes and regulations to provide the data and OEI has determined prior to the disclosure that OEI data handling requirements are satisfied. OEI may disclose limited individual identification information to another Federal agency for the purpose of matching and acquiring information held by that organization for OEI to use for the purposes stated for this system of records.

6. Contracts and Agreements. VA may disclose information from this system of records to individuals, organizations, private or public agencies, or other entities or

individuals with whom VA has a contract or agreement to perform such services as VA may deem practicable for the purposes of laws administered by VA, in order for the contractor, subcontractor, public or private agency, or other entity or individual with whom VA has a contract or agreement to perform services under the contract or agreement.

This routine use includes disclosures by an individual or entity performing services for VA to any secondary entity or individual to perform an activity that is necessary for individuals, organizations, private or public agencies, or other entities or individuals with whom VA has a contract or agreement to provide the service to VA.

This routine use, which also applies to agreements that do not qualify as contracts defined by Federal procurement laws and regulations, is consistent with OMB guidance in OMB Circular A-130, App. I, paragraph 5a(1)(b) that agencies promulgate routine uses to address disclosure of Privacy Act-protected information to contractors in order to perform the services contracts for the agency.

7. OMB. Any system records disclosure may be made to the OMB in order for them to perform their statutory responsibilities for evaluating Federal programs.

8. Outreach. Upon receipt of a written request, VA may disclose information to any state, tribe, county, or municipal agency for the purposes of outreach to a benefit under Title 38 Code of Federal Regulations (CFR).

9. Data breach response and remedial efforts. VA may, on its own initiative, disclose information from this system to appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that the integrity or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of embarrassment or harm to the reputations of the record subjects, harm to economic or property interests, identity theft or fraud, or harm to the security, confidentiality, or

integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the potentially compromised information; and (3) the disclosure is to agencies, entities, or persons whom VA determines are reasonably necessary to assist or carry out the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

This routine use permits disclosures by the Department to respond to a suspected or confirmed data breach, including the conduct of any risk analysis or provision of credit protection services as provided in 38 U.S.C. 5724.

10. Litigation. VA may disclose information from this system of records to the Department of Justice (DoJ), either on VA's initiative or in response to DoJ's request for the information, after either VA or DoJ determines that such information is relevant to DoJ's representation of the United States or any of its components in legal proceedings before a court or adjudicative body, provided that, in each case, the agency also determines prior to disclosure that release of the records to the DoJ is a use of the information contained in the records that is compatible with the purpose for which VA collected the records. VA, on its own initiative, may disclose records in this system of records in legal proceedings before a court or administrative body after determining that the disclosure of the records to the court or administrative body is a use of the information contained in the records that is compatible with the purpose for which VA collected the records.

To determine whether to disclose records under this routine use, VA will comply with the guidance promulgated by the Office of Management and Budget in a May 24, 1985,

memorandum entitled ‘‘Privacy Act Guidance—Update,” currently posted at http://www.whitehouse.gov/omb/inforeg/guidance1985.pdf

11. Law Enforcement. VA may, on its own initiative, disclose information in this system, except the names and home addresses of veterans and their dependents, which is relevant to a suspected or reasonably imminent violation of law, whether civil, criminal or regulatory in nature and whether arising by general or program statute or by regulation, rule or order issued pursuant thereto, to a Federal, state, local, tribal, or foreign agency charged with the responsibility of investigating or prosecuting such violation, or charged with enforcing or implementing the statute, regulation, rule or order. On its own initiative, VA may also disclose the names and addresses of veterans and their dependents to a Federal agency charged with the responsibility of investigating or prosecuting civil, criminal or regulatory violations of law, or charged with enforcing or implementing the statute, regulation, rule or order issued pursuant thereto.

**POLICIES AND PRACTICES FOR STORAGE OF RECORDS:**

OEI’s records are maintained electronically. Other electronic data is placed on VA’s segregated servers which are housed at VA’s Austin Information Technology Center, 615 Woodward St., Austin, TX, 78772. All imported and exported OEI data is handled and housed via the provisions of signed data use agreements and VA data security policies, procedures, and directives. Requestors of OEI stored information within VA, or from external individuals, contractors, organizations, and/or agencies with whom VA has a contract or agreement, must provide an equivalent level of security protection and comply with current VA policies and procedures for storage and transmission as codified in VA directives such as but not limited to VA Handbook 6500 and Directive 6513.

**POLICIES AND PRACTICES FOR RETRIEVABILITY OF RECORDS:**

OEI's records may be retrieved by using an individual's social security number, military service number, VA claim or file number, non-VA Federal benefit identifiers, and other personal identifiers.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:**

In accordance with 36 CFR 1234.34, *Destruction of Electronic Records*, "electronic records may be destroyed only in accordance with a records disposition schedule approved by the Archivist of the United States, including General Records Schedules." This office's electronic files are destroyed or deleted when no longer needed for administrative, legal, audit, or other operational purposes in accordance with records disposition authority approved by the Archivist.

If the Archivist has not approved disposition authority for any records covered by the system notice, the system manager will take immediate action to have the disposition of records in the system reviewed and paperwork initiated to obtain an approved records disposition authority in accordance with *VA Handbook 6300.1, Records Management Procedures*. The records may not be destroyed until VA obtains an approved records disposition authority. OEI will publish an amendment to this notice upon issuance of a NARA-approved disposition authority.

**PHYSICAL, PROCEDURAL AND ADMINISTRATIVE SAFEGUARDS**

All VA offices are protected from outside access by security personnel seven days a week. Entrances and exits are monitored by security cameras and protected by an alarm system. All VA staff and visitors are required to either have a VA-issued employment identification card or a temporary visitor identification badge. All work stations are secured during daytime and evening hours.

All data requests must be in writing, reviewed by a data review board, concurred on by the Executive Director for Data Governance and Analysis (DG&A) (008B), and released under the auspices of a signed data use agreement. File extracts provided for specific official uses will be limited to contain only the information fields needed for the analysis. Data used for analyses will have individual identifying characteristics removed or encrypted whenever possible. Unencrypted sensitive variables will only be used for analysis as a last resort.

Security complies with applicable Federal Information Processing Standards (FIPS) issued by the National Institute of Standards and Technology (NIST). Non-health information files containing unique identifiers such as social security numbers are encrypted to NIST-verified FIPS 140-2 standard or higher for storage, transport, or transmission. All files stored or transmitted on laptops, workstations, data storage devices and media are encrypted. Files are kept encrypted at all times except when data is in immediate use, per specifications by VA Office of Information and Technology. NIST publications were consulted in development of security for this system of records.

In the event of a contract or special project, VA may secure the services of contractors and/or subcontractors. In such cases, VA will maximize the use of encrypted data, when possible. Contractors and their subcontractors are required to maintain the same level of security as VA staff for non-health care information that has been disclosed to them. Unless explicitly authorized in writing by the VA, sensitive or protected data made available to the contractor and subcontractors shall not be divulged or made known in any manner to any person. All VA employees and contractors are mandated to complete annual cyber security and privacy training.

**SYSTEM MANAGER(S) AND ADDRESS (ES):** OEI's System Manager is Kshemendra Paul, Executive Director, Office of Enterprise Integration, Data Governance and

Analytics (008B1), VA Central Office, 810 Vermont Ave., NW. Washington, DC 20420, 202-461-1052, Kshemendra.Paul@va.gov.

**RECORD ACCESS PROCEDURE:** An individual (or duly authorized representative of such individual) who seeks access or wishes to contest records maintained under his or her name or other personal identifier may write or call the individuals listed under the Notification Procedure below.

**CONTESTING RECORD PROCEDURES:** (See Record Access Procedures above.)

**NOTIFICATION PROCEDURE:**

A Veteran who wishes to determine whether a record is being maintained by the Office of Enterprise Integration under his or her name or other personal identifier or wishes to determine the contents of such records should submit a written request or apply in person to: (1) Privacy Officer, or the Executive Director, Office of Enterprise Integration, Data Governance and Analytics (008B1), VA Central Office, 810 Vermont Ave., NW. Washington, DC 20420. Inquiries need to include the individual's full name and social security number.

**EXEMPTIONS PROMULGATED FOR THE SYSTEM:** None.

[FR Doc. 2021-01528 Filed: 1/22/2021 8:45 am; Publication Date: 1/25/2021]