performs backups for the Exec VA Application Server and the Oracle Database Server, respectively, according to the following schedule:

- Incremental data backups on a daily basis; and
- Full data backups on a weekly basis.

RETENTION AND DISPOSAL:

Records will be maintained and disposed of, in accordance with records disposition authority, approved by the Archivist of the United States.

SYSTEM MANAGER(S) AND ADDRESSES:

Director, Customer Relations & Executive Projects, Office of the Secretary, 810 Vermont Ave., NW., Washington, DC 20420; (202) 273–4830.

NOTIFICATION PROCEDURES:

Individuals seeking to determine whether this System of Records contains information, about them, should address written inquiries to the Office of Secretary (00), Department of Veterans Affairs, 810 Vermont Ave., NW., Washington, DC 20420. Requests should contain the full name, address and telephone number of the individual making the inquiry.

RECORD ACCESS PROCEDURE:

Individuals seeking to access or contest the contents of records, about themselves, contained in this System of Records should address a written request, including full name, address and telephone number to the Office of Secretary (00), Department of Veterans Affairs, 810 Vermont Ave., NW., Washington, DC 20420.

CONTESTING RECORD PROCEDURE:

(See Record Access Procedure above.)

RECORD SOURCE CATEGORIES:

Individuals who contact VA via the VA Web site at *http://www.va.gov* or by using a VA call center include veterans, veterans' family members and/or their representatives, government employees (Federal, State and local), realtors and home buyers, small business owners, vendors, funeral directors, clinicians, teachers, researchers, employees of veterans' service organizations, member of the public and all other individuals and representatives of organizations.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

No exemptions claimed for this system.

[FR Doc. E9–5599 Filed 3–13–09; 8:45 am]

BILLING CODE 8329–01–P

DEPARTMENT OF VETERANS AFFAIRS

Privacy Act of 1974; System of Records

AGENCY: Department of Veterans Affairs.

ACTION: Notice of publication of new system of records.

SUMMARY: The Privacy Act of 1974 (5 U.S.C. Section 552a) requires that all agencies publish in the **Federal Register** a notice of the existence of and character of their systems of records. Notice is hereby given that the Department of Veterans Affairs (VA) is adding a new system records entitled ''Inspector General Oversight Data Extracts—VA,'' (154VA53C).

DATES: Comments on this new system of records must be received not later than April 15, 2009. If no public comment is received, the amended system will become effective April 15, 2009.

ADDRESSES: Written comments may be submitted through *http://www.Regulations.gov*; by mail or hand-delivery to the Director, Regulations Management (02REG), Department of Veterans Affairs, 810 Vermont Ave., NW., Room 1068, Washington, DC 20420; or by fax to (202) 273–9026. 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 a.m. and 4:30 p.m. Monday through Friday (except holidays). Please call (202) 461–4902 for an appointment. In addition, during the comment period, comments may be viewed online through the Federal Docket Management System (FDMS).

FOR FURTHER INFORMATION CONTACT: Timothy J. McGrath, Attorney Advisor, Department of Veterans Affairs, Office of Inspector General (50C), 810 Vermont Avenue, NW., Washington, DC 20420; or fax comments to (202) 565–8667; or e-mail comments to *timothy.mcgrath@va.gov*.

SUPPLEMENTARY INFORMATION:

I. Description of the Proposed System of Records

The ''Inspector General Oversight Data Extracts—VA'' system of records is a collection of data, and extracts of data utilized by the Department of Veterans Affairs, Office of Inspector General (OIG) in performing its statutory mission under title 5 U.S.C. App. 3.

The OIG's mission is to detect and deter fraud, waste, abuse, and mismanagement of operations in the Department of Veterans Affairs. The OIG accomplishes that mission through various operational means including criminal investigations, audits, healthcare inspections, and other administrative reviews. OIG components may use various databases or extracts of those databases in furtherance of their investigation, project or review.

The database extracts are provided from master databases under the jurisdiction of the Department of Veterans Affairs, including, but not limited to, the Veterans Benefits Administration, Veterans Health Administration, and the National Cemetery Administration. Data extracts may also be from databases provided by the Department of Defense as well as other Federal and State agencies. When an OIG component begins an investigation, project, or review that requires the use or analysis of a particular database, the OIG Data Analysis Division (53CT) at the Consolidated Franchise Data Center in Austin, Texas will prepare an appropriate extract from a master database. To the fullest extent possible, the OIG component will use only the minimum amount of information required for the investigation, project or review. In appropriate cases, the Data Analysis Division will remove any personal identifying information before forwarding the data extract. This policy is designed as a security measure to control the type and amount of data being used and worked on.

These data extracts contain 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.*), claims processing codes and information (*e.g.*, disability compensation and pension award codes, *etc.*), and other VA and non-VA Federal information.

The information is retrievable by name, social security number, military service number, claim or file number, non-VA Federal benefit identifiers, and other personal identifiers. Consequently, a Privacy Act system of records must be established in order to protect this information.

II. Proposed Routine Use of Disclosures of Data in the System

VA is proposing to establish the following routine use disclosures of the information that will be maintained in the system.

1. Any records may be disclosed to appropriate agencies, entities, and persons under the following circumstances: When (1) it is suspected or confirmed that the security 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 or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure is made to such agencies, entities, and persons who are reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

2. 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 investigation 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.

3. Disclosure may be made to a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained.

4. Any system records disclosure may be made to the National Archives and Records Administration in records management inspections under title 44, U.S.C.

5. VA may disclose information from this system 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 OIG has determined prior to the disclosure that VA and OIG data handling requirements are satisfied.

6. Any system records may be disclosed 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 an agreement or contract to perform the services of the contract or agreement. This routine use includes disclosures by the individual or entity performing the service 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.

7. Any system records disclosure may be made to the Office of Management and Budget (OMB) in order for them to perform their statutory responsibilities for evaluating Federal programs.

8. VA OIG may disclose information in this system of records to the Department of Justice (DoJ), either on VA OIG's initiative or in response to DoJ's request for the information, after either VA OIG 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 disclosure of the records to the Department of Justice is a use of the information contained in the records that is compatible with the purpose for which VA collected the records. VA OIG, 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 OIG collected the records.

VA must be able to provide information to DoJ in litigation where the United States or any of its components is involved or has an interest. A determination would be made in each instance that under the circumstances involved, the purpose is compatible with the purpose for which VA collected the information. This routine use is distinct from the authority to disclose records in response to a court order under subsection (b)(11) of the Privacy Act, 5 U.S.C. 552(b)(11), or any other provision of subsection (b), in accordance with the court's analysis in *Doe* v. *DiGenova*, 779 F.2d 74, 78–84 (D.C. Cir. 1985) and *Doe* v. *Stephens*, 851 F.2d 1457, 1465–67 (D.C. Cir. 1988).

In determining 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*.

9. Disclosure to other Federal agencies may be made to assist such agencies in preventing and detecting possible fraud or abuse by individuals in their operations and programs.

III. Compatibility of the Proposed Routine Uses

The Privacy Act permits VA to disclose information about individuals without their consent for a routine use when the information will be used for a purpose that is compatible with the purpose for which we collected the information. In all of the routine use disclosures, either the recipient of the information will use the information in connection with a matter relating to one of VA's programs, or will use the information to provide a benefit to VA, or disclosure is required by law.

The ''notice of intent to publish'' and an advance copy of the system notice have been sent to the appropriate Congressional committees and the OMB's Director as required by 5 U.S.C. 552a(r) (Privacy Act) and guidelines issued by OMB on December 12, 2000 (65 FR 77677).

Approved: February 24, 2009.

John R. Gingrich,

Chief of Staff, Department of Veterans Affairs.

154VA53C

SYSTEM NAME:

Inspector General Oversight Data Extracts—VA.

SYSTEM LOCATION:

The location for electronic records is in the Office of Inspector General, Information Technology and Data Analysis Division, (53CT), U.S. Department of Veterans Affairs, Consolidated Franchise Data Center, 1615 Woodward Street, Austin, TX 78772.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

1. Service members and veterans who have applied for any type of benefits under title 38, U.S.C.

2. Veterans' spouse, surviving spouse, previous spouse, children, and parents who have applied for any type of benefit under title 38, U.S.C.

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

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

5. VA employees, contractor employees, and volunteers.

6. Employees of VA affiliated hospitals and medical schools, researchers, and without compensation (WOC) employees.

CATEGORIES OF RECORDS IN THE SYSTEM:

The records in this system of records consist of data, and extracts of data, provided from master databases under the jurisdiction of the Department of Veterans Affairs, including but not limited to, the Veterans Benefits Administration, Veterans Health Administration, and the National Cemetery Administration. Data extracts may also be from databases provided by the Department of Defense, as well as other Federal and State agencies. 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.), claims processing codes and information (*e.g.*, disability compensation and pension award codes, etc.), and other VA and non-VA Federal information.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Title 5, U.S.C. App. 3.

PURPOSE(S):

The records in this system of records are used for qualitative, quantitative, and other analyses used to support OIG reviews, investigations, audits, and healthcare inspections. The Inspector General has a statutory mission of detecting and preventing fraud, waste, abuse, and mismanagement in the Department of Veterans Affairs programs and operations and does so through a number of means. The OIG intends that its operational elements will utilize the least amount of data necessary to support a particular project or review.

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 health information protected by 45 CFR parts 160 and 164 and 38 U.S.C. 7332, that information cannot be disclosed under any of the following routine uses unless there is also specific statutory authority in 38 U.S.C. 7332 and regulatory authority in 45 CFR parts 160 and 164 permitting disclosure.

1. Any records may be disclosed to appropriate agencies, entities, and persons under the following circumstances: When (1) it is suspected or confirmed that the security 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 or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure is made to such agencies, entities, and persons who are reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such. 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.

2. 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.

3. Disclosure may be made to a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained.

4. Any system records disclosure may be made to the National Archives and Records Administration in records management inspections under title 44, U.S.C.

5. VA may disclose information from this system to a Federal agency to conduct 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 OIG has determined prior to the disclosure that VA and OIG data handling requirements are satisfied.

6. Any system records may be disclosed 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 an agreement or contract to perform the services of the contract or agreement. This routine use includes disclosures by the individual or entity performing the service 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.

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

8. VA OIG may disclose information in this system of records to the Department of Justice (DoJ), either on VA OIG's initiative or in response to DoJ's request for the information, after either VA OIG 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 disclosure of the records to the Department of Justice is a use of the information contained in the records that is compatible with the

purpose for which VA OIG collected the records. VA OIG, 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 OIG collected the records. In determining whether to disclose records under this routine use, VA OIG 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*.

9. Disclosure to other Federal agencies may be made to assist such agencies in preventing and detecting possible fraud or abuse by individuals in their operations and programs.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

The Department will not make disclosures from this system of records to consumer reporting agencies.

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

STORAGE:

OIG's records in this system of records are maintained in an electronic format on VA's segregated server housed at VA's Consolidated Franchise Data Center, 1615 Woodward Street, Austin, TX 78772. Access to that electronic data is handled through the OIG's Data Analysis Division (53CT). All imported and exported OIG data is handled and housed via the provisions of current VA and OIG data security policies, procedures, and directives.

RETRIEVABILITY:

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

SAFEGUARDS:

Access to the server in the Consolidated Franchise Data Center in Austin, TX is limited by appropriate locking devices and restricted to authorized VA personnel. The Consolidated Franchise Data Center is a secure facility protected by a variety of physical and electronic safeguards.

The OIG will publish internal guidance and policy for its employees concerning requests for data extracts to support a project or review. A written request identifying and justifying the use of the data will be necessary. File extracts provided for specific official uses will be limited to contain only the information fields needed for the project or review. Further, only authorized individuals may have access to the data and only when needed to perform their official duties. Whenever possible, data used for analyses will have individual identifying characteristics removed or encrypted.

Security complies with applicable Federal Information Processing Standards (FIPS) issued by the National Institute of Standards and Technology (NIST). 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 the VA Office of Information Technology. NIST publications were consulted in development of security for this system of records.

Access to data storage areas is restricted to authorized VA and OIG employees, or contract staff who have been cleared to work by the VA Office of Security and Law Enforcement. File areas are locked after normal duty hours. VA facilities are protected from outside access by the Federal Protective Service and/or other security personnel.

In the event of a contract or special project, OIG may secure the services of contractors and/or subcontractors. In such cases, OIG will maximize the utilization of encrypted data, when possible. Contractors and their subcontractors are required to maintain the same level of security as VA and OIG staff for sensitive VA information that has been disclosed to them. Unless explicitly authorized in writing by the OIG, 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 OIG employees and contractors are mandated to complete annual cyber security and privacy training.

RETENTION AND DISPOSAL:

In accordance with Title 36, CFR, Section 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.'' The OIG'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. OIG will publish an amendment to this notice upon issuance of a NARA-approved disposition authority.

SYSTEM MANAGER(S) AND ADDRESS(ES):

OIG's system manager is the Director, Information Technology and Data Analysis Division, (53CT), Office of Inspector General, U.S. Department of Veterans Affairs, 1615 Woodward Street, Austin, TX 78772.

NOTIFICATION PROCEDURE:

An individual who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or wants to determine the contents of such record, should submit a written request to the Director, Information Technology and Data Analysis Division, (53CT) Office of Inspector General, U.S. Department of Veterans Affairs, 1615 Woodward Street, Austin, TX 78772. Such requests must contain a reasonable description of the records requested. In addition, identification of the individual requesting the information will be required in the written request and will minimally consist of the requester's name, signature, social security number, address, telephone number, and return address.

RECORD ACCESS PROCEDURES:

(See Notification procedure above.)

CONTESTING RECORDS PROCEDURES:

(See Notification procedure above.)

RECORD SOURCE CATEGORIES:

This system of records information is obtained from VA's databases, the Department of Defense, Federal and State agencies, and other organizations whose data is necessary to accomplish the purpose for this system of records.

[FR Doc. E9–5603 Filed 3–13–09; 8:45 am]

BILLING CODE 8320–01–P