

or seeking additional information should contact Ms. Farber at (202) 461-9728 or Ersie.farber@va.gov.

Dated: July 22, 2009.

By Direction of the Secretary.

E. Philip Riggins,

Committee Management Officer.

[FR Doc. E9-17907 Filed 7-27-09; 8:45 am]

BILLING CODE P

DEPARTMENT OF VETERANS AFFAIRS

Privacy Act; Systems of Records

AGENCY: Department of Veteran Affairs (VA).

ACTION: Notice of establishment of new system of records.

SUMMARY: The Privacy Act of 1974 (5 U.S.C. 552a (e) (4)) requires that all agencies publish in the **Federal Register** a notice of the existence and character of their system of records. Notice is hereby given that the Department of Veterans Affairs (VA) is establishing a new system of records entitled "Veterans Information Solution (VIS)—VA" (137VA005Q).

DATES: Comments on this new system of records must be received no later than August 27, 2009. If no public comment is received, the new system will become effective August 27, 2009.

ADDRESSES: Written comments may be submitted through <http://www.Regulations.gov>; by mail or hand-delivery to the Director, Regulations Management (00REG), Department of Veterans Affairs, 810 Vermont Avenue, NW., Room 1063B, 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: David Lindsey, Program Manager, VADIR, Registration and Eligibility (005Q3), 810 Vermont Avenue, NW., Washington, DC 20420; telephone (202) 245-1679.

SUPPLEMENTARY INFORMATION:

a. Description of Proposed System of Records

VIS is an Intranet-based application that provides a consolidated view of information gathered from the

Beneficiary Identification and Record Locator Subsystem (BIRLS), the Veterans Affairs/Department of Defense Identity Repository (VADIR), the Benefits Delivery Network (BDN), and the Rating Board Automation (RBA2000) corporate database for determination of eligibility for veteran's benefits. VIS provides a read only view of a subset of the data contained within these databases listed; VIS does not provide updates to any of these systems, nor does it retain any of the data gathered from these systems. Once the user request has been fulfilled, the data is expunged from the system.

b. Proposed Routine Use Disclosures of Data in the System

VA is proposing to establish the following Routine Use disclosures of data accessed by the VIS application from the identified data sources:

1. The record of an individual included in this system may be provided to Department of Defense (DoD) systems or offices for use in connection with matters relating to one of DoD's programs to enable delivery of healthcare or other DoD benefit to eligible beneficiaries.

2. The name, address, VA file number, effective date of compensation or pension, current and historical benefit pay amounts for compensation or pension, service information, date of birth, competency payment status, incarceration status, and social security number of veterans and their surviving spouses may be disclosed to the Department of Defense Manpower Data Center (DMDC) to reconcile the amount and/or waiver of service, department and retired pay. These records may also be disclosed as part of a computer matching program to accomplish these purposes.

3. The name, address, VA file number, date of birth, date of death, social security number, and service information may be disclosed to DoD's DMDC. DoD will use this information to identify retired veterans and dependent members of their families who have entitlement to Department of Defense benefits but who are not identified in the Department of Defense Enrollment Eligibility Reporting System (DEERS) program and to assist in determining eligibility for Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) benefits. This purpose is consistent with 38 U.S.C. 5701.

4. VA may disclose on its own initiative any information in this system, except the names and addresses of veterans and their dependents, that 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, 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. VA may also disclose on its own initiative 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.

5. VA may disclose any information or records to appropriate agencies, entities, and persons when (1) it is suspected or confirmed that the integrity or confidentiality of information in the system of records has been compromised; (2) VA 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 records subjects, harm to economic or property interest, identity theft or fraud, or harm to the security, confidentiality or integrity of this system or other systems or programs (whether maintained by VA or another agency or entity) that rely upon the potentially compromised information; and (3) the disclosure is made to such agencies, entities, and persons whom VA determines are reasonably necessary to assist or carry out VA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm. This routine use permits disclosures by VA to respond to a suspected or confirmed data breach, including the conduct of any risk analysis or provision or credit protection services as provided in 38 U.S.C. 5724, as the terms are defined in 38 U.S.C. 5727.

6. 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.

7. The record of an individual who is covered by a system of records may be disclosed to a Member of Congress, or a staff person acting for the member, when the member or staff person requests the record on behalf of and at the written request of the individual.

8. The name(s) and address(es) of a veteran may be disclosed to another Federal agency or to a contractor of that agency, at the written request of the

head of that agency or designee of the head of that agency for the purpose of conducting government research necessary to accomplish a statutory purpose of that agency.

9. VA may disclose information in the 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 records to the DOJ is a use of 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.

10. Where VA determines that there is good cause to question the legality or ethical propriety of the conduct of a person or organization representing a person in a matter before VA, a record from this system may be disclosed, on VA's initiative, to any or all of the following: (1) Applicable civil or criminal law enforcement authorities and (2) a person or entity responsible for the licensing, supervision, or professional discipline of the person or organization acting as representative. Name and home addresses of veterans and their dependents will be released on VA's initiative under this routine use only to Federal entities when VA believes that the names and addresses are required by the Federal department or agency.

11. Disclosure of relevant information may be made 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 or entity or individual with whom VA has an agreement or contract to perform the services of the contract or agreement.

12. Disclosure may be made to the National Archives and Records Administration or the General Services Administration in records management inspections conducted under authority of Title 44 U.S.C.

c. Search Capability—Users may only gain access to the VIS application if they provide a valid user ID, password, and station number. Upon successful login and authentication to the VIS application, users are provided a search screen. Search criteria may include either name or one of the following numeric entries: SSN, File Number, and Service Number.

d. Sensitive Records—The VIS application notifies users when an attempt is made in violation of sensitivity levels. These notifications occur when an authorized user attempts to view the veteran information that has a higher sensitivity level ranking than he or she has been granted.

e. Design Constraints—The VIS system sits within the Austin Automation Center in Austin, Texas; therefore it must conform to the requirements and standards established for those environments. This includes requirements such as access control to the systems, revision/patch levels for hardware operating systems and database management systems, and use of security tools such as antivirus software, intrusion detection software and spyware.

f. Certification & Accreditation—The VIS system has gone through the Certification & Accreditation (C&A) process. During this process, the system underwent a series of risk and security assessments and had extensive documentation developed to support the integrity of the system. The VA C&A process is used to certify that the VIS system has adequate logical, management and technical security controls in place that minimize the system's risk to unauthorized access and disclosure.

g. Privacy Impact Assessment—The VIS system has had a comprehensive Privacy Impact Assessment conducted on it to ensure that the privacy of the information contained within the system is adequately protected according to VA and Office of Management and Budget (OMB) privacy and security standards.

h. Internal Communications Architecture—Information is requested by VIS from the VADIR, BIRLS, BDN and RBA2000 systems and displayed for the requestor. All data transmissions associated with these data requests are over the internal VA network using approved security protocols to protect the data.

i. Compatibility of the Proposed Routine Uses—The Privacy Act permits the VA to disclose information about the individuals contained in a system of records without their consent for a routine use, when the information will

be used for a purpose that is compatible with the purpose for which the information was collected. In all of the routine use disclosures described above, either the recipient of the information will use the information in connection with a matter relating to one of VA's programs, to provide a benefit to the veteran, or disclosure is required by law. The notice of intent to publish an advance copy of the system notice has been sent to the appropriate Congressional committees and to the Director of OMB as required by 5 U.S.C. 552a(r) (Privacy Act) and guidelines issued by OMB (65 FR 77677), December 12, 2000.

Approved: July 10, 2009.

John R. Gingrich,

Chief of Staff, Department of Veterans Affairs.

137VA005Q

SYSTEM NAME:

“Veterans Information Solution (VIS)—VA” (137VA005Q).

SYSTEM LOCATION:

The VIS application is located in the Austin Automation Center (AAC), 1615 East Woodward Street, Austin, Texas 78772. A second VIS disaster recovery site is planned to be stood up in FY09 at the Veterans Affairs (VA) data center in Hines, Illinois.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The category of the individuals covered by the VIS application include Veterans and their dependents whose information is provided to VIS via the Beneficiary Identification and Record Locator Subsystem (BIRLS), the Veterans Affairs/Department of Defense Identity Repository (VADIR), the Benefits Delivery Network (BDN), and the Rating Board Automation (RBA2000) corporate database.

CATEGORIES OF RECORDS IN THE SYSTEM:

The record, or information contained in the record, may include identifying information (e.g., name, address, social security number); military service and active duty separation information (e.g., name, service number, date of birth, rank, sex, total amount of active service, branch of service, character of service, pay grade, assigned separation reason, whether Veteran was discharged with a disability, types of disabilities, served in Vietnam Conflict, reenlisted, received a Purple Heart or other military decoration); personal information (e.g., marital status, name and address of dependents, occupation, amount of education of a Veteran or a dependent, dependent's relationship to Veteran).

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Title 38, United States Code, Part II, Chapters 11, 13, 15, 17, 18, 19 and 23.

PURPOSE:

VIS is an Intranet-based application that provides a consolidated view of information gathered from the BIRLS, VADIR, BDN, and RBA2000 systems for determination of eligibility for Veteran's benefits. VIS provides a read only view of a subset of the data contained within these databases listed; VIS does not provide updates to any of these systems, nor does it retain any of the data gathered from these systems. Once the user request has been fulfilled, the data is expunged from the system.

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

1. The record of an individual included in this system may be provided to Department of Defense (DoD) systems or offices for use in connection with matters relating to one of DoD's programs to enable delivery of healthcare or other DoD benefit to eligible beneficiaries.

2. The name, address, VA file number, effective date of compensation or pension, current and historical benefit pay amounts for compensation or pension, service information, date of birth, competency payment status, incarceration status, and social security number of Veterans and their surviving spouses may be disclosed to the Department of Defense Manpower Data Center (DMDC) to reconcile the amount and/or waiver of service, department and retired pay. These records may also be disclosed as part of a computer matching program to accomplish these purposes.

3. The name, address, VA file number, date of birth, date of death, social security number, and service information may be disclosed to DoD's DMDC. DoD will use this information to identify retired Veterans and dependent members of their families who have entitlement to Department of Defense benefits but who are not identified in the Department of Defense Enrollment Eligibility Reporting System (DEERS) program and to assist in determining eligibility for Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) benefits. This purpose is consistent with 38 U.S.C. 5701.

4. VA may disclose on its own initiative any information in this system, except the names and addresses of Veterans and their dependents, that 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, 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. VA may also disclose on its own initiative 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.

5. VA may disclose any information or records to appropriate agencies, entities, and persons when (1) it is suspected or confirmed that the integrity or confidentiality of information in the system of records has been compromised; (2) VA 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 records subjects, harm to economic or property interest, identity theft or fraud, or harm to the security, confidentiality or integrity of this system or other systems or programs (whether maintained by VA or another agency or entity) that rely upon the potentially compromised information; and (3) the disclosure is made to such agencies, entities, and persons whom VA determines are reasonably necessary to assist or carry out VA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm. This routine use permits disclosures by VA to respond to a suspected or confirmed data breach, including the conduct of any risk analysis or provision or credit protection services as provided in 38 U.S.C. 5724, as the terms are defined in 38 U.S.C. 5727.

6. 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.

7. The record of an individual who is covered by a system of records may be disclosed to a Member of Congress, or a staff person acting for the member, when the member or staff person requests the record on behalf of and at the written request of the individual.

8. The name(s) and address (es) of a veteran may be disclosed to another Federal agency or to a contractor of that agency, at the written request of the head of that agency or designee of the

head of that agency for the purpose of conducting government research necessary to accomplish a statutory purpose of that agency.

9. VA may disclose information in the system of records to the Department of Justice (DOJ), either on VA's initiative or in response to DOJ's request for 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, or in a proceedings before a court or adjudicative body provided that, in each case, the agency also determines prior to disclosure that release of records to the DOJ is a use of 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.

10. Where VA determines that there is good cause to question the legality or ethical propriety of the conduct of a person or organization representing a person in a matter before VA, a record from this system may be disclosed, on VA's initiative, to any or all of the following: (1) Applicable civil or criminal law enforcement authorities and (2) a person or entity responsible for the licensing, supervision, or professional discipline of the person or organization acting as representative. Name and home addresses of Veterans and their dependents will be released on VA's initiative under this routine use only to Federal entities when VA believes that the names and addresses are required by the Federal department or agency.

11. Disclosure of relevant information may be made 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 or entity or individual with whom VA has an agreement or contract to perform the services of the contract or agreement.

12. Disclosure may be made to the National Archives and Records Administration or the General Services Administration in records management inspections conducted under authority of Title 44 U.S.C.

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

The VIS application electronically stores personal information on veterans only long enough to fulfill a user's request for information; once the user's request is fulfilled, the data is expunged from the system.

RETRIEVABILITY:

The VIS application queries the BIRLS, the VADIR, the BDN, and the RBA2000 corporate database to populate user requests for data. The data is retrieved using name, social security number, and/or other unique personal identifier.

SAFEGUARDS:

1. Physical Security: The VIS system is located in the AAC in Texas; a backup disaster recovery system will be installed at the Hines Data Processing Center in Illinois. Access to data processing centers is generally restricted to center employees, custodial personnel, Federal Protective Service and other security personnel. Access to computer rooms is restricted to authorized operational personnel through electronic locking devices. All

other persons needing access to computer rooms are escorted.

2. System Security: Access to the VA network is protected by the usage of "logon" identifications and passwords. Once on the VA network, separate ID and password credentials are required to gain access to the VIS server and/or database. Access to the server and/or database is granted to a limited number of users, system administrators and database administrators. In addition VIS has undergone certification and accreditation. Based on a risk assessment that followed National Institute of Standards and Technology Vulnerability and Threat Guidelines, the system is considered stable and operational and an Authority to Operate has been granted. The system was found to be operationally secure, with very few exceptions or recommendations for change.

RETENTION AND DISPOSAL:

The VIS Application does not retain veteran's personal data in the application system. VIS queries four data systems (BIRLS, VADIR, BDN and RBA2000) to meet user requests for data; once the user request has been satisfied, the data is expunged from the system.

SYSTEM MANAGER(S) AND ADDRESSES:

The official responsible for maintaining the VADIR repository: Program Manager, Registration and Eligibility, Office of Enterprise Development, Interagency Program Executive Office (005Q3), ATTN: VIS System of Records, 810 Vermont Avenue, NW., Washington, DC 20420.

NOTIFICATION PROCEDURES:

Individuals seeking information on the existence and content of a record pertaining to them should contact the system manager, in writing, at the above address. Requests should contain the full name, address and telephone number of the individual making the inquiry.

RECORD ACCESS PROCEDURE:

See Notification Procedure above.

CONTESTING RECORD PROCEDURES:

See Notification Procedure above.

RECORD SOURCE CATEGORIES:

The VIS data sources are: VADIR, the BIRLS, the BDN, and the RBA2000 corporate database.

[FR Doc. E9-17910 Filed 7-27-09; 8:45 am]

BILLING CODE 8320-01-P