DEPARTMENT OF VETERANS AFFAIRS

Privacy Act of 1974; System of Records

AGENCY: Department of Veterans Affairs (VA).

ACTION: Notice of Amendment to System of Records.

SUMMARY: As required by the Privacy Act of 1974, 5 U.S.C. 552a(e), notice is hereby given that the Department of Veterans Affairs (VA) is amending the system of records currently titled "Income Verification Records-VA" (89VA16) as set forth in the Federal Register (73 FR 26192- 26197), dated May 8, 2008. VA is amending the System Number, System Location, Access, Routine Uses of Records Maintained in the System, Storage, Safeguards, and Records Source Categories. VA is republishing the system notice in its entirety.

DATES: Comments on the amendment of this system of records must be received no later than **[Insert date 30 days after date of publication in the Federal Register]**. If no public comment is received, the amended system will become effective **[Insert date 30 days after date of publication in the Federal Register]**.

ADDRESSES: Written comments may be submitted through www.Regulations.gov; by mail or hand-delivery to Director, Regulations Management (02REG), Department of Veterans Affairs, 810 Vermont Avenue, NW., Room 1068, Washington, DC 20420; or by fax to (202) 273-9026. 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. In addition, during the comment period, comments may be viewed online through the Federal Docket Management System at www.Regulations.gov.

FOR FURTHER INFORMATION CONTACT: Veterans Health Administration Privacy Officer, Department of Veterans Affairs, 810 Vermont Avenue, NW., Washington, DC 20420; telephone (704) 245-2492.

SUPPLEMENTARY INFORMATION:

BACKGROUND

Public Law 101-508, the Omnibus Budget Reconciliation Act of 1990, provides VA the authority to verify Veterans' self-reported income to determine eligibility for medical benefits. VA's Health Eligibility Center (HEC) in Atlanta, Georgia, originally established as the Income Verification Match Center, has authority under section 8051 to verify Veterans' self-reported income with the Internal Revenue Service (IRS) and Social Security Administration (SSA).

The system number is changed from 89VA16 to 89VA10NB to reflect the current organizational alignment.

The System Location, Access, and Safeguard sections have been amended to change the Austin Automation Center to what is now known as the Austin Information Technology Center.

Routine use nineteen (19) has been added to state that disclosures 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.

The section titled ‘‘Storage’’ is being amended to state that records are maintained at a secure off-site facility in Atlanta and Austin. In January 2013, VA implemented a new electronic data transmission process called Direct Connect, which is a secure Virtual Private Network (VPN) tunnel to transmit and receive Veterans' household income from IRS. VPN only affects the means in which the data is transmitted; it does not affect the storage of the data.

“Safeguard” is being amended under number three (3) to include that the card has restricted access capability, which allows restriction of unauthorized personnel to secured areas. HEC Security Officer has been replaced with HEC Personal Card Issuer. Number twelve (12) has been amended to replace the Center with the HEC Information Security Office (ISO).

The section titled ‘‘Records Source Categories’’ has been amended to change 24VA19 to 24VA10P2 and “Compensation, Pension, Education and Rehabilitation Records—VA’’ (58VA21/22) to “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA” (58VA21/22/28).

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.

Approved: December 2, 2013.

Jose D. Riojas, Chief of Staff,

Department of Veteran Affairs.

[8320-01]

SOR #: 89VA10NB

SYSTEM NAME: "Income Verification Records-VA"

SYSTEM LOCATION: Records are maintained at VA's Health Eligibility Center (HEC) in Atlanta, Georgia, and the Austin Information Technology Center (AITC) in Austin, Texas. Records are also stored at contracted locations in McLean, Virginia, and Atlanta, Georgia.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Veterans who have applied for or have received VA health care benefits under Title 38, United States Code, Chapter 17; Veterans' spouses and other dependents as provided for in other provisions of Title 38, United States Code.

CATEGORIES OF RECORDS IN THE SYSTEM: The category of records in the system includes:

Federal Tax Information (FTI) and social security information generated as a result of computer matching activity with records from the IRS and SSA. The records may also include, but are not limited to, correspondence between HEC, Veterans, their family members, and Veterans' representatives such as Veterans Service Officers (VSO); copies of death certificates; Notice of Separation; disability award letters; IRS documents (e.g., Form 1040s, Form 1099s, W-2s); workers compensation forms; and various annual earnings statements, as well as pay stubs and miscellaneous receipts.

Note: VA may not disclose to any person in any manner any document that contains FTI received from IRS or SSA in accordance with the Internal Revenue Code (IRC) 26 U.S.C. 6103(l)(7). In addition, VA may not allow access to FTI by any contractor or subcontractor.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317.

PURPOSE(S): Information in this system of records is used to verify the household income of certain Veterans and, if relevant, their spouses or dependents receiving VA health care benefits. The information in this system of records is also used to validate Veterans' and their spouses' social security numbers; provide educational materials related to income verification; respond to Veteran and non-Veteran inquiries related to income verification; and compile management reports.

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

To the extent that records contained in the system include information protected by 45 CFR Parts 160 and 164, (i.e., individually identifiable health information and 38 U.S.C. 7332), (i.e., medical treatment information related to drug abuse, alcoholism or alcohol abuse, sickle cell anemia or infection with the human immunodeficiency virus), that information cannot be disclosed under a routine use 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. VA may disclose the record of an individual who is covered by this system to a member of Congress or staff person acting for the member in response to an inquiry made at the request of that individual.

2. VA may disclose any information in this system of records, except FTI, as deemed necessary and proper to named individuals serving as accredited service organization representatives and other individuals named as approved agents or attorneys for a

documented purpose, period of time, or specific income year, to aid beneficiaries in the preparation and presentation of their cases during the verification and/or due process procedures and in the presentation and prosecution of claims under laws administered by VA.

3. VA may disclose, on its own initiative, any information in this system, except the names, home addresses, or FTI 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, 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. Additionally, 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.

4. VA may disclose relevant information in this system, except FTI, in the course of presenting evidence to a court, magistrate, or administrative tribunal; in matters of guardianship, inquests, and commitments; to private attorneys representing Veterans rated incompetent in conjunction with issuance of Certificates of Incompetency; and to probation and parole officers in connection with court-required duties.

5. VA may disclose information in this system, except FTI, to a VA Federal fiduciary or a guardian ad litem in relation to his or her representation of a Veteran in any legal proceeding, but only to the extent necessary to fulfill the duties of the fiduciary or the

guardian ad litem.

6. VA may disclose relevant information in this system, except FTI, to attorneys, insurance companies, employers, third parties liable or potentially liable under health plan contracts, and to courts, boards, or commissions, but only to the extent necessary to aid VA in the preparation, presentation, and prosecution of claims authorized under Federal, State, or local laws, and regulations promulgated there under.

7. VA may disclose information in 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 disclosure of the records to 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.

8. VA may disclose any information in this system, except FTI, to National Archives and Records Administration (NARA) and General Services Administration in records management inspections conducted under Title 44 of United States Code.

9. VA may disclose information in this system, except FTI, to a third party, except consumer reporting agencies, in connection with any proceeding for the collection of an amount owed to the United States by virtue of a person's participation in any benefit

program administered by VA, but only to the extent that it is reasonably necessary to (a) assist VA in the collection of costs of services provided individuals not entitled to such services; and (b) initiate civil or criminal legal actions for collecting amounts owed to the United States and/or for prosecuting individuals who willfully or fraudulently obtained or seek to obtain Title 38 medical benefits. This disclosure is consistent with 38 U.S.C. 5701(b)(6).

10. VA may disclose the names and addresses of Veterans or their dependents and other information as is reasonably necessary to identify such individuals concerning that those individuals' indebtedness to the United States by virtue of their participation in a benefits program administered by VA to a consumer reporting agency for purposes of assisting in the collection of such indebtedness, provided that the provisions of 38 U.S.C. 5701(g)(4) have been met.

11. VA may disclose information from this system, except FTI, or information security review purposes to other source Federal agencies who are parties to computer matching agreements involving the information maintained in this system, but only to the extent that the information is necessary and relevant to the review.

12. VA may disclose the name and other identifying information of Veterans and their spouses to reported payers of earned or unearned income in order to verify the identifier address, income paid, period of employment, and health insurance information provided on the means test, and to confirm income and demographic data provided by other Federal agencies during income verification computer matching.

13. VA may disclose identifying information other than FTI, such as Veterans' and their dependents' social security numbers, to other Federal agencies for purposes of

conducting computer matches to obtain valid identifying, demographic, and income information and to verify eligibility of certain Veterans who are receiving VA medical benefits under Title 38, United States Code, or for the purpose of conducting a computer match to obtain information to validate social security numbers maintained in VA records.

14. VA may disclose the name and social security number of a Veteran, spouse, and dependents, and other identifying information as is reasonably necessary to the SSA and the Department of Health and Human Services, for the purpose of conducting a computer match to obtain information to validate the social security numbers maintained in VA records.

15. VA may disclose relevant information from this system to individuals, organizations, private or public agencies, etc., 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 or subcontractor to perform the services of the contract or agreement.

Note: This routine use does not authorize disclosure of FTI received from the IRS or the SSA to contractors or subcontractors.

16. VA may, on its own initiative, disclose any information or records 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) 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 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 VA 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 VA 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 of credit protection services as provided in 38 U.S.C. 5724, as the terms are defined in 38 U.S.C. 5727.

17. VA may disclose information to officials of the Merit Systems Protection Board, or the Office of Special Counsel, when requested 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 may be authorized by law.

18. VA may disclose information to the Federal Labor Relations Authority (including its General Counsel) information related to the establishment of jurisdiction, the investigation and resolution of allegations of unfair labor practices, or information in connection with the resolution of exceptions to arbitration awards when a question of material fact is raised; to disclose information in matters properly before the Federal Services Impasses Panel, and to investigate representation petitions and conduct or supervise representation elections.

19. 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.

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

STORAGE: Records are currently maintained on magnetic tape, magnetic disk, optical disk, and paper at secure off-site facilities in Atlanta, Georgia, and Austin, Texas. In January 2013, VA implemented a new electronic data transmission process called Direct Connect, which is a secure VPN tunnel to transmit and receive Veterans' household income from IRS. It only affects the means in which the data is transmitted; it does not affect the storage of the data.

RETRIEVABILITY: Records (or information contained in records) maintained on paper documents are indexed and accessed by the applicant's name, social security number or case number and filed in case order number. Automated records are indexed and retrieved by the Veteran's name, social security number, Internal Control Number, or case number. The spouse's name or social security number may be retrieved from the automated income verification record.

ACCESS:

1. In accordance with national and locally established data security procedures, access to the HEC Legacy system and the Enrollment Database is controlled by unique entry codes (access and verification codes). The user's verification code is set to be changed automatically every 90 days. User access to data is controlled by role-based access as determined necessary by supervisory and information security staff as well as by

management of option menus available to the employee. Determination of such access is based upon the role or position of the employee and functionality necessary to perform the employee's assigned duties.

2. On an annual basis, employees are required to sign a computer access agreement acknowledging their understanding of confidentiality requirements. In addition, all employees receive annual privacy awareness and information security training. Access to electronic records is deactivated when no longer required for official duties. Recurring monitors are in place to ensure compliance with nationally and locally established security measures.

3. Access to the AITC is generally restricted to AITC staff, VA Headquarters employees, custodial personnel, Federal Protective Service, and authorized operational personnel through electronic locking devices.

4. Specific key staffs are authorized access to HEC computer room and all other persons gaining access to the computer rooms are escorted. Programmer access to the information systems is restricted only to staff whose official duties require that level of access.

SAFEGUARDS:

1. Electronic data transmissions between VA health care facilities, HEC, and AITC are safeguarded by using VA's secure wide area network. The transmission of electronic data between SSA and AITC is safeguarded through the use of a secured, encrypted connection. Back-up of magnetic media containing FTI is transported between AITC and the off-site location in a locked storage container by an off-site vendor. Vendor personnel do not have key access to the locked container. The locked storage

container is stored in a safe in a secured room at the off-site storage location. Access to the secured room and the safe is limited to authorized VA Information Technology staff only.

2. The software programs at HEC, AITC, and VA health care facilities automatically flag records or events for transmission via electronic messages based upon functionality requirements. The recipients of the messages are controlled and/or assigned to the mail group based on their role or position. Server jobs at each facility run continuously to check for incoming and outgoing data to be transmitted which needs to be parsed to files on the receiving end. All messages containing data transmissions include header information that is used for validation purposes. Consistency checks in the software are used to validate the transmission, and electronic acknowledgment messages are returned to the sending application. The VA Office of Cyber Security has oversight responsibility for planning and implementing computer security.

3. Working spaces and record storage areas at the HEC are secured during all business hours, as well as during non-business hours. All entrance doors require an electronic pass card, issued by the HEC Personal Card Issuer, for entry when unlocked, and entry doors are locked outside normal business hours. The card has restricted access capability, which allows restriction of unauthorized personnel to secured areas. Visitors are required to present identification and sign-in at a specified location. Visitors are issued a pass card which allows access to non-sensitive areas and are escorted by staff through restricted areas. At the end of the visit, visitors are required to turn in their card. The building is equipped with an intrusion alarm system which is activated during non-business hours. This alarm system is monitored by a private security service

vendor. The HEC office space occupied by employees with access to Veteran records is secured with an electronic locking system, which requires a card for entry and exit of that office space. Access to the AITC is generally restricted to AITC staff, VA Headquarters employees, custodial personnel, Federal Protective Service, and authorized operational personnel through electronic locking devices. All other persons gaining access to the computer rooms are escorted.

4. A number of other security measures are implemented to enhance security and safeguard of electronic records such as automatic timeout after a short period of inactivity and device locking after a pre-set number of invalid logon attempts, for example.

5. Electronic data, except FTI, is transmitted from HEC and AITC to VA health care facilities over VA secure wide area network.

6. Employees at the health care facility level do not have access to FTI, nor do they have the ability to edit or view income tests received from HEC as a result of the income match with IRS.

7. Only specific key staff and the ISO are authorized access to the computer room. Programmer access to AITC and HEC databases, which contain FTI, is restricted only to staff whose official duties require that level of access. Contractor staff are not authorized access to the production database.

8. On-line data, including FTI, reside on magnetic media in AITC computer room which are highly secured. Backup media are stored in a combination lock safe in a secured room within the same building and access to the safe is restricted to the IT staff. Backup media are stored by an off-site media storage vendor who picks up the media

on a weekly basis from HEC and AITC and returns the media to the off-site storage via a locked storage container. Vendor personnel do not have key access to the locked container.

9. Any sensitive information that may be downloaded to a personal computer or printed to hard copy format is provided the same level of security as the electronic records. All paper documents and informal notations containing sensitive data are shredded prior to disposal. All magnetic media (primary computer system) and personal computer disks are degaussed prior to disposal or released off site for repair.

10. HEC and AITC fully comply with the Tax Information Security Guidelines for Federal, State and Local Agencies (Department of Treasury IRS Publication 1075) as it relates to access and protection of such data. These guidelines define the management of magnetic media, paper and electronic records, and physical and electronic security of the data.

11. All new HEC employees receive initial information security and privacy training and refresher training are provided to all employees on an annual basis. HEC's ISO performs an Annual Information Security (AIS) audit. This annual audit includes the primary computer information system, the telecommunication system, and local area networks. Additionally, the IRS performs periodic on-site inspections to ensure the appropriate level of security is maintained for FTI. HEC and AITC's ISO and AIS administrator additionally perform periodic reviews to ensure security of the system and databases.

12. Identification codes and codes used to access HEC automated communications systems and records systems, as well as security profiles and possible security

violations, are maintained on magnetic media in a secure environment by the HEC ISO. For contingency purposes, database back-ups on removable magnetic media are stored off-site by a licensed and bonded media storage vendor.

13. VA field facilities do not receive FTI from AITC or HEC.

14. Contractors and subcontractors are required to adhere to HEC's safeguard and security requirements.

RETENTION AND DISPOSAL: Depending on the record medium, records are destroyed by either shredding or degaussing. Paper records are destroyed after they have been accurately scanned on optical disks. Optical disks or other electronic medium are deleted when all phases of the Veteran's appeal rights have ended (10 years after the income year for which the means test verification was conducted). Electronic data and magnetic media received at AITC from SSA and IRS are destroyed 30 days after the data have been validated as being a true copy of the original data. Summary reports and other output reports are destroyed when no longer needed for current operation. Records are disposed of in accordance with the records retention standards approved by the Archivist of the United States, NARA, and published in the Veterans Health Administration Records Control Schedule 10-1. Regardless of the record medium, no records will be retired to a Federal records center.Vet

SYSTEM MANAGER(S) AND ADDRESS: Official responsible for policies and procedures: Chief Business Office (10NB2A), VA Central Office, 810 Vermont Avenue, NW., Washington, DC 20420. Official maintaining the system: Director, Health Eligibility Center, 2957 Clairmont Road, Atlanta, Georgia, 30329.

NOTIFICATION PROCEDURE: Any 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 or apply in person to the Health Eligibility Center. All inquiries must reasonably identify the records requested. Inquiries should include the individual's full name, social security number, and return address.

RECORD ACCESS PROCEDURES: Individuals seeking information regarding access to and contesting of income verification records may write to the Director, Health Eligibility Center, 2957 Clairmont Road, Suite 200, Atlanta, Georgia, 30329.

CONTESTING RECORD PROCEDURES:

(See Record Access Procedures above.)

RECORD SOURCE CATEGORIES: Information in this systems of records may be provided by the applicant, applicant's spouse or other family members; accredited representatives or friends; employers and other payers of earned income; financial institutions and other payers of unearned income; health insurance carriers; other Federal agencies; the “Patient Medical Records—VA” (24VA10P2) and the “Enrollment and Eligibility Records—VA” (147VA16) systems of records; and Veterans Benefits Administration (VBA) automated record systems (including the “Veterans and Beneficiaries Identification and Records Location Subsystem-VA” (38VA23) and the “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA” (58VA21/22/28)).

[FR Doc. 2013-30228 Filed 12/18/2013 at 8:45 am; Publication Date: 12/19/2013]