

veteran records is secured with an electronic locking system, which requires a card for entry and exit of that office space. Access to the AAC is generally restricted to AAC staff, VA Central Office 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.

3. Access to the VIC contractor secured work areas is also controlled by electronic entry devices, which require a card and manual input for entry and exit of the production space. The VIC contractor's building is also equipped with an intrusion alarm system and a security service vendor monitors the system.

4. Contract employees are required to sign a Business Associates Agreement (BAA) as required by the Health Insurance Portability and Accountability Act of 1996 as acknowledgement of mandatory provisions regarding the use and disclosure of protected health information. Employee and contractor access is deactivated when no longer required for official duties or upon termination of employment. Recurring monitors are in place to ensure compliance with nationally and locally established security measures.

5. Beneficiary's enrollment and eligibility information is transmitted from the Enrollment and Eligibility information system to VA health care facilities over the Department's secure computerized electronic communications system.

6. Only specific key staff have authorized access to the computer room. Programmer access to the information systems is restricted only to staff whose official duties require that level of access.

7. On-line data reside on magnetic media in the HEC and AAC computer rooms that are highly secured. Backup media are stored in the computer room within the same building and only information system staff and designated management staff have access to the computer room. On a weekly basis, backup media are stored in off-site storage by a media storage vendor. The vendor picks up and returns the media in a locked storage container; vendor personnel do not have key access to the locked container. The AAC has established a backup plan for the Enrollment system as part of a required Certification and Accreditation of the information system.

8. Any sensitive information that may be downloaded to personal computers 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 release off-site for repair. The VIC contractor destroys all veteran identification data 30 days after the VIC card has been mailed to the veteran in accordance with contractual requirements.

9. All new HEC employees receive initial information security and privacy training; refresher training is provided to all employees on an annual basis. The HEC's Information Security Officer performs an annual information security audit and periodic reviews to ensure security of the system. 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 Federal tax data.

10. Identification codes and codes used to access Enrollment and Eligibility information systems and records systems, as well as security profiles and possible security violations, are maintained on magnetic media in a secure environment at the Center. For contingency purposes, database backups on removable magnetic media are stored off-site by a licensed and bonded media storage vendor.

11. Contractors, subcontractors, and other users of the Enrollment and Eligibility Records systems will adhere to the same safeguards and security requirements to which HEC staff must comply.

RETENTION AND DISPOSAL:

Regardless of the record medium, all records are disposed of in accordance with the records retention standards approved by the Archivist of the United States, National Archives and Records Administration, and published in the VHA Records Control Schedule 10-1.

SYSTEM MANAGER(S) AND ADDRESSES:

Official responsible for policies and procedures: Chief Business Officer (16), VA Central Office, 1722 I St., 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, military service number, claim folder number and return address.

RECORD ACCESS PROCEDURES:

Individuals seeking information regarding access to and contesting of Enrollment and Eligibility Records may write to the Director, Health Eligibility Center, 2957 Clairmont Road, Atlanta, Georgia 30329.

CONTESTING RECORD PROCEDURES:

(See Record Access procedures above).

RECORD SOURCE CATEGORIES:

Information in the systems of records may be provided by the applicant; applicant's spouse or other family members or accredited representatives or friends; health insurance carriers; other Federal agencies; "Patient Medical Records—VA" (24VA19) system of records; "Veterans Health Information System and Technology Architecture (VistA) Records—VA" (79VA19); "Income Verification Records—VA" (89VA19); and Veterans Benefits Administration automated record systems, including "Veterans and Beneficiaries Identification and Records Location Subsystem—VA" (38VA23) and the "Compensation, Pension, Education and Rehabilitation Records—VA" (58VA21/22).

[FR Doc. E8-5956 Filed 3-24-08; 8:45 am]

BILLING CODE 8320-01-P

DEPARTMENT OF VETERANS AFFAIRS

Privacy Act of 1974

AGENCY: Department of Veterans Affairs.

ACTION: Notice of new system of records.

SUMMARY: The Privacy Act of 1974 (5 U.S.C. 552(e)(4)) requires that all agencies publish in the **Federal Register** a notice of the existence and character of their systems of records. Notice is hereby given that the Department of Veterans Affairs (VA) is establishing a new system of records entitled "Department of Veterans Affairs Personnel Security File System (VAPSFS)"—(145VA005Q3).

DATES: Comments on this new system of records must be received no later than April 24, 2008. If no public comment is received, the new system of records will

become effective 30 days after publication of this Notice.

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 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 (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 (FDMS) at www.Regulations.gov.

FOR FURTHER INFORMATION CONTACT: VA Personal Identity Verification (PIV) Program Manager, VA PIV Program Office, Veterans Affairs Central Office, 810 Vermont Avenue, Room B11, Washington, DC 20420, (202) 461-9759 (This is not a toll free number).

SUPPLEMENTARY INFORMATION:

I. Description of the Proposed System of Records

The PIV Applicant may be a current or prospective Federal hire, a Federal employee, contractor, or affiliate who requires routine, long-term logical access to VA information or information systems, and/or physical access to VA facilities to perform their jobs. An affiliate is defined as a non-Federal employee or contract individual. Examples of affiliates include students, researchers, residents, veteran service organization volunteers, temporary help, interns, individuals authorized to perform or use services provided in VA facilities, and individuals formerly in any of these positions. At its discretion, VA may include short-term employees and contractors in the PIV program; therefore, these records are included in the system of records. VA shall make risk-based decisions to determine whether to issue PIV cards and to require prerequisite background checks for short-term employees, contractors, and affiliates. As required by FIPS 201, this system of records addresses VA's collection of individually-identified biographic and biometric information from the PIV Applicant in order to conduct the required PIV background investigation or other national security investigations. VA is promulgating this system of records following OMB Directive M-05-24 guidance in accordance with 5 U.S.C. a(v) in the

performance of providing Privacy Act guidance to Federal agencies.

The PIV background investigation matches the PIV Applicant's information against Department of Justice (DOJ), Federal Bureau of Investigation (FBI), Office of Personnel Management (OPM), and VA databases to prevent the hiring of applicants with a disqualifying criminal record, or other disqualifying issues such as severe financial problems, drug or alcohol abuse, or possible affiliations with unlawful entities, that may result in an unfavorable background adjudication. If persons decline to provide information required to conduct a background investigation, VA will not issue them a PIV card. Two forms are used to initiate the background investigation: Questionnaire for Non-Sensitive Positions Standard Form 85 (SF-85) or the Questionnaire for National Security Positions Standard Form 86 (SF-86). This background investigation process entails collecting the PIV Applicant's fingerprints, conducting a Special Agency Check (SAC), and may also include a National Agency Check with Inquires (NACI), which are described below:

SAC: Pursuant to an agreement between VA and OPM or DOJ, a SAC consists of a fingerprint search of criminal history records by the Federal Bureau of Investigation (FBI), Criminal Justice Information Services Division. Each SAC also includes a check of OPM's Suitability/Security Investigation Index (SII). The SAC is also referred to as the Fingerprint only check.

NACI: The basic and minimum investigation required on all new Federal employees consisting of searches of the OPM Security/Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII), the Federal Bureau of Investigation (FBI) Identification Division's name and fingerprint files, and other files or indices when necessary, with written inquiries and searches of records covering specific areas of an individual's background during the past 5 years.

The biographic, biometric, and background information collected as part of this PIV card enrollment process and its results are kept in secure personnel and background investigation files, for which this system of records shall manage.

A separate, yet related system of records addresses the personal data collection for the remainder of the PIV enrollment process—the VA Identity Management System (VAIDMS)—which completes the identity proofing and

registration and card issuance operations. The PIV Applicant presents PIV-compliant identity documents, demographic data, employment data, facial image, and fingerprints to create a data record in the VAIDMS. Together these two systems of records will collect and manage the appropriate information to allow a PIV card to be issued to authorized VA employees, contractors, or affiliates, and to effectively manage the PIV card throughout its life cycle operations.

II. Proposed Routine Use Disclosures of Data in the System

1. Disclosure 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, 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.

2. VA may disclose the information listed in 5 U.S.C. 7114(b)(4) to officials of labor organizations recognized under 5 U.S.C. Chapter 71 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

3. VA may disclose the information to officials of the Merit Systems Protection Board, or the Office of the 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.

4. VA may disclose the information to the Equal Employment Opportunity Commission when requested in connection with investigations of alleged or possible discriminatory practices, examination of Federal affirmative employment programs, or for other functions of the Commission as authorized by law or regulation.

5. VA may disclose the 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.

6. VA may disclose the information 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.

7. VA may disclose the information to the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906.

8. VA may disclose information in this system of records to DOJ and OPM, either on VA's initiative or in response to DOJ's and OPM's request for the information, after either VA, DOJ, or OPM determines that such information is relevant to OPM's or 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 or OPM 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.

9. VA may disclose the information, except as noted on Forms SF 85, 85-P, and 86, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether Federal, foreign, State, local, or tribal, or otherwise, responsible for enforcing, investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant

thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative or prosecutorial responsibility of the receiving entity.

10. VA may disclose the information to a Federal, State, local, foreign, or tribal or other public authority the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative personnel or regulatory action.

11. VA may disclose on its own initiative any 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.

III. Compatibility of the Proposed Routine Uses

Release of information from these records pursuant to routine uses will be made only in accordance with the provisions of the Privacy Act of 1974. The Privacy Act of 1974 permits agencies 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 the information was collected. In the routine use disclosures proposed for this new VA system of records, VA will disclose individually-identified information for the following purposes: In connection with VA's administrative notice and rulemaking process, to

contractors to perform a function associated with that process, for law-enforcement activities, and in administrative and judicial proceedings. The VA has determined that the disclosure of information for the above purposes is a proper and necessary use of the information collected by the VAPSFS system, and is compatible with the purpose for which VA collected the information.

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 OMB as required by 5 U.S.C. 552a(r) (Privacy Act), as amended, and guidelines issued by OMB (65 FR 77677), December 12, 2000.

Approved: March 11, 2008.

Gordon H. Mansfield,

Deputy Secretary of Veterans Affairs.

145VA005Q3

SYSTEM NAME:

Department of Veterans Affairs
Personnel Security File System
(VAPSFS).

SYSTEM LOCATION:

Primary location: Paper records are kept at the individual VA field site locations, within the local Department of Human Resources offices, as well as the Security and Investigations Center (SIC), at Little Rock, AR. Secondary locations: Electronic records are kept at the VA Data Centers at Falling Waters, WV, Hines, IL, Austin Automation Center, Austin, TX, and at the SIC, Little Rock, AR.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who require routine, long-term access to VA federal facilities, and/or information technology systems to perform their jobs. VA employees, contractors, and affiliates are covered by the system of records. An affiliate is defined as a non-Federal employee or contract individual. Examples of affiliates include students, researchers, residents, veteran service organization volunteers, temporary help, interns, individuals authorized to perform or use services provided in VA facilities, and individuals formerly in any of these positions. At their discretion, VA may include short-term employees and contractors in the PIV program and, therefore, these records are included in the system of records. VA shall make risk-based decisions to determine whether to issue PIV cards and to require prerequisite background checks for short-term employees, contractors, and affiliates. The system also includes

individuals accused of security violations or found in violation by VA security officials.

CATEGORIES OF RECORDS IN THE SYSTEM:

Information is obtained from a variety of sources including the employee, contractor, or applicant via use of the SF-85, SF-85P, SF-86, and personal interviews; employers' and former employers' records; DOJ, FBI, OPM, DOD criminal history records and other databases; background investigation Case Number (CN), Social Security Number (SSN), fingerprints, financial institutions and credit reports; medical records and health care providers; educational institutions; interviews of witnesses such as neighbors, friends, co-workers, business associates, teachers, landlords, or family members; tax records; and other public records. VA security violation information is obtained from a variety of sources, such as guard reports, security inspections, witnesses, supervisor's reports, and audit reports.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The U.S. government is authorized to ask for this information under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive 12.

PURPOSE:

The records in this system of records are used to document background and security investigation information which support decisions as to the eligibility and fitness for service of VA PIV applicants for VA employment and contract positions, and may include employees, contractors, and affiliates, to the extent their duties require access to VA federal facilities and/or information systems. They may also be used to document security violations and supervisory actions taken in response to those violations.

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

1. Disclosure 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, 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.

2. VA may disclose the information listed in 5 U.S.C. 7114(b)(4) to officials of labor organizations recognized under 5 U.S.C. Chapter 71 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

3. VA may disclose the information to officials of the Merit Systems Protection Board, or the Office of the 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.

4. VA may disclose the information to the Equal Employment Opportunity Commission when requested in connection with investigations of alleged or possible discriminatory practices, examination of Federal affirmative employment programs, or for other functions of the Commission as authorized by law or regulation.

5. VA may disclose 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.

6. VA may disclose the information 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.

7. VA may disclose the information to the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906.

8. VA may disclose information in this system of records to the Department

of Justice (DOJ) and OPM, either on VA's initiative or in response to DOJ's and OPM's request for the information, after either VA, DOJ, or OPM determines that such information is relevant to OPM's or 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 DOJ or OPM 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.

9. VA may disclose the information, except as noted on Forms SF 85, 85-P, and 86, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether Federal, foreign, State, local, or tribal, or otherwise, responsible for enforcing, investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative or prosecutorial responsibility of the receiving entity.

10. VA may disclose the information to a Federal, State, local, foreign, or tribal or other public authority the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another Federal agency for criminal, civil, administrative personnel or regulatory action.

11. VA may disclose on its own initiative any 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 STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records are stored on paper and electronically in secure VA locations.

RETRIEVABILITY:

Background investigation records are retrieved by case number (CN), name, Social Security Number (SSN), or fingerprint.

SAFEGUARDS:

For paper records: Comprehensive paper records are kept in locked metal file cabinets in locked rooms at the field site Department of Human Resources offices, and the SIC, Little Rock, AR. The paper records are maintained in controlled facilities where physical entry is restricted by the use of locks, guards, and administrative procedures. Access to the records is limited to those employees who have a need for them in the performance of their official duties. In addition, all personnel whose official duties require access to the information have undergone appropriate background investigations and are trained and certified in the proper safeguarding and use of the information.

For electronic records: Electronic records pertaining to any background investigation data collected during the PIV enrollment process are kept in the PIV Identity Management System maintained at VA Data Centers in Falling Waters, WV; Hines, IL; Austin Automation Data Center, Austin, TX; and at the SIC, Little Rock, AR. Electronic records are maintained in a secure, password protected electronic system that utilizes security hardware and software to include: Encryption, multiple firewalls, active intruder

detection, and role-based access controls.

Access to the records is restricted to those with a specific role in the PIV administrative process that requires access to background investigation forms to perform their duties, and who have been given authorization and password to access that part of the system. An audit trail is maintained and reviewed periodically to identify attempts to access, and actual unauthorized access events. Persons given roles in the PIV process have undergone appropriate background investigations and must complete training and be certified in their specific roles to ensure they are knowledgeable about how to protect sensitive and individually-identified information.

RETENTION AND DISPOSAL:

These records are retained and disposed of in accordance with General Records Schedule 18, item 22, approved by the National Archives and Records Administration (NARA). Records are destroyed upon notification of death or not later than five years after separation or transfer of employee, whichever is applicable.

SYSTEM MANAGER AND ADDRESS:

VA PIV Program Manager, Office of Information and Technology (005Q3), Department of Veterans Affairs, 810 Vermont Ave., NW., Room B-11, Washington, DC 20420; telephone (202) 461-9759 (This is not a toll free number).

NOTIFICATION PROCEDURES:

An individual can determine if this system contains a record pertaining to him/her by sending a signed written request to the Systems Manager. When requesting notification of or access to records covered by this Notice, an individual should provide his/her full name, date of birth, agency name, and work location. An individual requesting notification of records in person must provide identity documents sufficient to satisfy the custodian of the records that the requester is entitled to access, such as a government-issued photo ID. Individuals requesting notification via mail or telephone must furnish, at minimum, name, date of birth, social security number, and home address in order to establish identity.

RECORD ACCESS PROCEDURE:

Same as notification procedures.

CONTESTING RECORD PROCEDURE:

Same as notification procedures. Requesters should also reasonably identify the record, specify the information they are contesting, state

the corrective action sought and the reasons for the correction along with supporting justification showing why the record is not accurate, timely, relevant, or complete.

RECORD SOURCE CATEGORIES:

Information is obtained from a variety of sources including the employee, contractor, or affiliate applicant via use of the SF-85, SF-85P, or SF-86 and personal interviews; employer's and former employers' records; FBI criminal history records and other databases; financial institutions and credit reports; medical records and health care providers; educational institutions; interviews of witnesses such as neighbors, friends, co-workers, business associates, teachers, landlords, or family members; tax records; and other public records. VA security violation information is obtained from a variety of sources, such as guard reports, security inspections, witnesses, supervisor's reports, and audit reports.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Upon publication of a final rule in the **Federal Register**, this system of records will be exempt in accordance with 5 U.S.C. 552a(k)(5). Information will be withheld to the extent it identifies witnesses promised confidentiality as a condition of providing information during the course of the background investigation.

[FR Doc. E8-5969 Filed 3-24-08; 8:45 am]

BILLING CODE 8320-01-P

DEPARTMENT OF VETERANS AFFAIRS

Privacy Act of 1974

AGENCY: Department of Veterans Affairs.
ACTION: Notice of amendment to system of records.

SUMMARY: As required by the Privacy Act of 1974 (5 U.S.C. 552(e)(4)), notice is hereby given that the Department of Veterans Affairs (VA) is amending the system of records currently entitled, "Department of Veterans Affairs Federal Docket Management System (VAFDMS)—(140VA00REG)" as set forth in the **Federal Register** on February 9, 2007. VA is amending the system by revising the routine uses of records maintained in the system, including categories of users and the purpose of such uses. 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 April 24, 2008. If no public