relevant to a refusal to grant access privileges to automated veterans claims records, or a potential or past suspension or termination of such access privileges may be disclosed to the entity employing the individual to represent veterans on claims for veterans benefits.

60. The name and address of a former accredited representative, claim agent or attorney, and any information concerning such individual, except a veteran's name and home address, which is relevant to a revocation of such access privileges may be disclosed to an appropriate governmental licensing organization where VA determines that the individual's conduct which resulted in revocation merits reporting.

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

STORAGE:

Records (or information contained in records) are maintained on paper documents in claims file folders (e.g., "C" file folders, educational file folders and vocational rehabilitation folders) and on automated storage media (e.g., microfilm, microfiche, magnetic tape and disks). Such information may be accessed through a data telecommunication terminal system designated the Benefits Delivery Network (BDN). BDN terminal locations include VA Central Office, regional offices, some VA health care facilities, Department of Defense Finance and Accounting Service Centers and the U.S. Coast Guard Pay and Personnel Center.

Remote on-line access is also made available to authorized representatives of claimants and to attorneys of record for claimants. A VA claimant must execute a prior written consent or a power of attorney authorizing access to his or her claims records before VA will allow the representative or attorney to have access to the claimant's automated claims records. Access by representatives and attorneys of record is to be used solely for the purpose of assisting an individual claimant whose records are accessed in a claim for benefits administered by VA.

Information relating to receivable accounts owed to VA, designated the Centralized Accounts Receivable System (CARS), is maintained on magnetic tape, microfiche and microfilm. CARS is accessed through a data telecommunications terminal system at St. Paul, Minnesota.

* * * * *

RETREIVABILITY:

The proposed change should have no effect upon the current RETREIVABILITY policies or practices.

SAFEGUARDS:

1. Physical Security: (a) Access to working spaces and claims folder file storage areas in VA regional offices and centers is restricted to VA employees on a need-to-know basis. Generally, file areas are locked after normal duty hours and the offices and centers are protected from outside access by the Federal Protective Service or other security personnel. Employee claims file records and claims file records of public figures are stored in separate locked files. Strict control measures are enforced to ensure that access to and disclosure from these claims file records are limited to a needto-know basis.

(b) Access to BDN data telecommunications network is by authorization controlled by the site security officer who is responsible for authorizing access to the BDN by a claimant's representative or attorney approved for access in accordance with VA regulations. The site security officer is responsible for ensuring that the hardware, software and security practices of a representative or attorney satisfy VA security requirements before granting access. The security requirements applicable to access to automated claims files by VA employees also apply to access to automated claims files by claimants' representatives or attorneys. The security officer is assigned responsibility for privacysecurity measures, especially for review of violation logs, information logs and control of password distribution, including password distribution for claimants' representatives.

(c) 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 provided access to computer rooms are escorted.

(d) Employee production records are identified by the confidential BDN access number, not name, and are protected by management/supervisory personnel from unauthorized disclosure in the same manner as other confidential records maintained by supervisors.

2. *BDN System Security:* (a) Usage of the BDN system is protected by the usage of "logan" identification passwords and authorized function passwords. The passwords are changed periodically. These same protections apply to remote access users.

(b) At the data processing centers, identification of magnetic tapes and disks containing data is rigidly enforced using labeling techniques. Automated storage media which are not in use are stored in tape libraries which are secured in locked rooms. Access to programs is controlled at three levels: Programming, auditing and operations. Access to the data processing centers where HUD maintains CAIVRS is generally restricted to center employees and authorized subcontractors. Access to computer rooms is restricted to center employees and authorized operational personnel through electronic locking devices. All other persons granted access to computer rooms are escorted.

Files in CAIVRS use social security numbers as identifiers. Access to information files is restricted to authorized employees of participating agencies and authorized employees of lenders who participate in the agencies' programs. Access is controlled by agency distribution of passwords. Information in the system may be accessed by use of a touch-tone telephone by authorized agency and lender employees on a "need-to-know" basis.

* * * *

Report of Intention to Alter Federal Notice of System of Records for "Compensation, Pension, Education and Rehabilitation Records—VA" 58 VA 21/22

Purpose

Amending this system of records will allow VA to use information maintained by this system of records to be used to revoke the access of claimant's representatives to the system of records for violation of the provisions of 38 CFR 14.640 through 14.643.

Authority

Regulations 38 CFR 14.640 through 14.643.

Probable or Potential Effect on the Privacy of Individuals

These changes should have minimal effect on the privacy rights of individuals. They will permit VA to use information contained in this system of records to revoke access to this system to representatives of claimants who violate the provisions of regulations 38 CFR 14.640 through 14.643.

Steps Taken to Minimize Risks

VA will safeguard individual records as required by the Privacy Act of 1974. Access to working areas and claims