component information, and incident information. It may also take the form of an electronic VOQ containing the same information as identified above, which can be submitted via NHTSA's Internet Web site or by calling the Department of Transportation's Auto Safety Hotline. Or, it may take the form of a consumer letter. All consumer complaint information, in addition to other sources of available information, is entered into the agency's database and reviewed by NHTSA staff to determine whether a safety-related defect trend or catastrophic failure is developing that would warrant the opening of a safety defect investigation.

Affected Public: Individuals and households.

Estimated Total Annual Burden: 8,657 hours.

ADDRESSES: Send comments, within 30 days, to the Office of Information and Regulatory Affairs, Office of Management and Budget, 725–17th Street, NW., Washington, DC 20503, Attention NHTSA Desk Officer.

Comments Are Invited on: Whether the proposed collection of information is necessary for the proper performance of the functions of the Department, including whether the information will have practical utility; the accuracy of the Department's estimate of the burden of the proposed information collection; ways to enhance the quality, utility, and clarity of the information to be collected; and ways to minimize the burden of the collection of information on respondents, including the use of automated collection techniques or other forms of information technology.

Kathleen DeMeter,

Director, Office of Defects Investigation.

[FR Doc. E8–6181 Filed 3–25–08; 8:45 am]

BILLING CODE 4910–59–M

DEPARTMENT OF TRANSPORTATION

Pipeline and Hazardous Materials Safety Administration

[Docket No. PHMSA–RSPA–2004–19856]

Pipeline Safety: Issues Related to Mechanical Couplings Used in Natural Gas Distribution Systems

AGENCY: Pipeline and Hazardous Materials Safety Administration (PHMSA), DOT.

ACTION: Notice; Issuance of Advisory Bulletin; Corrections.

SUMMARY: PHMSA published a document in the **Federal Register** of March 4, 2008, issuing an advisory bulletin concerning failures of mechanical couplings and related appurtenances in natural gas distribution systems. The document described certain affected pipe incorrectly and did not clearly identify the State involved in certain data.

FOR FURTHER INFORMATION CONTACT: Richard Sanders at (405) 954–7214, or by e-mail at *richard.sanders@dot.gov*; or Max Kieba at (202) 493–0595, or by e-mail at *max.kieba@dot.gov*.

SUPPLEMENTARY INFORMATION:

Corrections

1. Because of the variations in the nature of the incidents and the approaches taken to them, PHMSA intended to describe separately the incidents and studies done in various states. In order to clarify the separation in the bulletized lists of incidents and studies, in the **Federal Register** of March 4, 2008, in FR Doc. E8–4155 correct the preamble text by adding a bullet symbol (•) in the following places:

a. On page 11696, in the second column, before the sentence ''Between 1980 and 2007, seven incidents occurred in Texas.''

b. On page 11697, in the first column, before the sentence ''A number of other studies, tests, and repair, or replacement programs, some of them voluntary, have been conducted in other States.''

2. In the **Federal Register** of March 4, 2008, in FR Doc. E8–4155, on page 11697, in the second column, in item 4 of the advisory bulletin, correct the description of the affected pipe in the first sentence to read ''pipe sizes between ½-inch CTS (Copper Tube Size) and two-inch IPS (Iron Pipe Size)''.

Issued in Washington, DC, on March 20, 2008.

William Gute,

Deputy Associate Administrator for Pipeline Safety.

[FR Doc. E8–6155 Filed 3–25–08; 8:45 am]

BILLING CODE 4910–60–P

DEPARTMENT OF VETERANS AFFAIRS

Privacy Act of 1974; System of Records

AGENCY: Department of Veteran 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 Identity Management System (VAIDMS)''—(146VA005Q3).

DATES: Comments on this new system of records must be received no later than April 25, 2008. If no public comment is received, the new system of records will become effective April 25, 2008.

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 (This is not a toll free number). 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 *http://www.Regulations.gov.*

FOR FURTHER INFORMATION CONTACT: VA PIV Program Manager, VA PIV Program Office, Department of Veterans Affairs, 810 Vermont Avenue, NW., Washington, DC 20420, (202) 461–9759 (This is not a toll free number).

SUPPLEMENTARY INFORMATION:

I. Description of the Proposed System of Records

The Department of Veterans Affairs Identity Management System (VAIDMS) is proposing to establish a system of records that will be used to ensure that access to Federal facilities and information is restricted to authorized individuals, in accordance with Homeland Security Presidential Directive 12 (HSPD–12), which requires Federal agencies to issue uniform identification cards to eligible Federal employees and contractors and directed the National Institute of Standards and Technology (NIST) to establish a new standard for these Personal Identity Verification (PIV) cards. To comply with the directive, VA will collect, manage, and retrieve individually-identified personal information pertaining to VA employees, contractors, and affiliates who require routine, long-term logical access to VA information or information systems, and/or physical access to VA facilities to perform their jobs. Affiliates include students, researchers, residents,

Veterans 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. VA is promulgating this system of records following Office of Management and Budget (OMB) Directive M–05–24 guidance in accordance with 5 U.S.C. 552a(v) in the performance of providing Privacy Act guidance to Federal agencies.

The PIV card enrollment data collection process requires the applicant to provide two PIV-compliant identity documents to confirm the individual's identity. In addition, the PIV applicant's facial image and fingerprints are also captured to create a data record in the PIV Identity Management System.

HSPD–12 and the standards promulgated by NIST require that the PIV card be secure and reliable, enhance security, increase efficiency, reduce identity fraud, and protect personal privacy. HSPD–12 established four control objectives for Federal agencies to accomplish in implementing the directive:

- Issue identification credentials based on sound criteria to verify an individual's identity;
- Issue credentials that are strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation;
- Provide for rapid, electronic authentication of personal identity; and
- Issue credentials by providers whose reliability has been established through an official accreditation process.

The scope of the VA PIV Program consists of PIV card enrollment services collecting PIV applicant data; a fully integrated VA PIV systems infrastructure using a centralized VA Identity Management System (VAIDMS); and related card registration, card issuance, and card management operations.

The VA PIV enrollment process and data collection will cover all VA employees, contractors, and affiliates who require routine, long-term access to VA facilities, and information systems. The personal information collected during the enrollment process consists of data and records necessary to verify the identity of the individual applying for the PIV card. VA may, at its discretion, 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. The VAIDMS will collect data elements from the PIV card applicant, including full legal name, date of birth, Social Security number, organizational and employee affiliations, fingerprints, digital color photograph, work e-mail address, and phone number(s), as well additional verification and demographic information. A Card Holder Unique Identifier (CHUID) is also developed and stored in the system of records by combining several of these collected data elements to create a specific individually-identified data element uniquely linked to the PIV card holder.

A separate, yet related system of records, the VA Personnel Security File System (VAPSFS), handles PIV applicant background investigation data collection and management prior to the PIV card enrollment process. VAPSFS captures pertinent background history and fingerprint information from the PIV applicant. This background investigation effort is conducted in order to determine the eligibility of an applicant to obtain a PIV card for accessing VA resources. 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

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

This routine use includes agreements that are not considered contracts under Federal procurement law. In addition, it is consistent with OMB guidance in OMB Circular A–130, App. I, paragraph 5a(1)(b) that agencies promulgate routine uses to address disclosure of Privacy Act-protected information to contractors in order to perform the services contracts for the agency.

2. 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) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of embarrassment or harm to the reputations of the record subjects, harm to economic or property interests, identity theft or fraud, or harm to the security, confidentiality, or integrity of this system or other systems or programs (whether maintained by the Department 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 in or carry out the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

This routine use permits disclosures by the Department to respond to a suspected or confirmed data breach, including the conduct of any risk analysis or provision of credit protection services as provided in 38 U.S.C. 5724, as the terms are defined in 38 U.S.C. 5727.

VA's ability to respond quickly and effectively in the event of a breach of Federal data is critical to its efforts to prevent or minimize any consequent harm. An effective response necessitates disclosure of information regarding the breach to those individuals affected by it, as well as to persons and entities in a position to cooperate, either by assisting in notification to affected individuals or playing a role in preventing or minimizing harms from the breach.

3. 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.

VA must be able to provide information to unions to assist them in advancing workers' interests with respect to wages, benefits, and working conditions. This routine use does not provide the unions with any greater access to Privacy-Act-protected

information than access under section 7114(b) to information that is not protected by the Privacy Act. It simply removes the Privacy Act as a bar to the disclosure of the information at the agency's discretion.

4. VA may disclose the information to officials of the Merit Systems Protection Board (MSPB), 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.

VA must be able to provide information to MSPB for it to perform duties imposed by statutes and regulations.

5. VA may disclose the information to the Equal Employment Opportunity Commission, (EEOC) 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.

VA must be able to provide information to EEOC for it to perform duties imposed by statutes and regulations.

6. VA may disclose the information to the Federal Labor Relations Authority (FLRA) 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.

VA must be able to provide information to FLRA for it to perform duties imposed by statutes and regulations.

7. 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.

VA must be able to provide information about individuals to adequately respond to inquiries from Members of Congress at the request of constituents who have sought their assistance.

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

VA must be able to disclose information to NARA and GSA to comply with statutory requirements to disclose information to these agencies for them to perform their records management duties.

9. VA may disclose information in this system of records to the Department of Justice (DOJ) and Office of Personnel Management (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 DOJ's or OPM's representation of the United States or any of its components in legal proceedings before a court or adjudicative body, provided that, in each case, the agency also determines prior to disclosure that disclosure of the records to the Department of Justice 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.

10. 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.

VA must be able to provide on its own initiative information that pertains to a violation of laws to law enforcement authorities in order for them to investigate and enforce those laws. Under 38 U.S.C. 5701(a) and (f), VA may only disclose the names and addresses of veterans and their dependents to Federal entities with law enforcement responsibilities. This is distinct from the authority to disclose records in response to a qualifying request from a law enforcement entity, as authorized by Privacy Act subsection 5 U.S.C. 552a(b)(7).

III. Compatibility of the Proposed Routine Uses

Release of information from these records 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, the recipient of the information will use the information in connection with a matter relating to one of VA's programs, will use the information to provide a benefit to VA, 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 the Office of Management and Budget (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 12, 2008.

Gordon H. Mansfield,

Deputy Secretary of Veterans Affairs.

146VA005Q3

SYSTEM NAME:

Department of Veterans Affairs Identity Management System (VAIDMS)

SYSTEM LOCATION:

Primary location: Electronic records are kept at the VA Data Center at Falling Waters, WV. Secondary locations: VA Data Center at Hines, IL, and Austin Automation Center, Austin, TX. Paper records are kept at the individual VA field site locations, within the local human resources offices.

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, namely:

1. VA employees;

2. Contractors and subcontractors;

3. Affiliates, including students, researchers, residents, Veterans Service Organization volunteers, temporary help, and interns.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records maintained, on individuals issued PIV cards by VA, include the following data fields: Full legal name, Social Security number; date of birth; signature; facial image (photograph); fingerprints; hair color; eye color; height; weight; organization/office of assignment; company name; telephone number; Personal Identity Verification (PIV) card issue and expiration dates; personal identification number (PIN); results of background investigation; PIV card request form; PIV registrar approval signature; PIV card serial number; PIV card expiration date; copies of documents used to verify PIV card applicant identification, and/or information derived from those documents, such as document title, document issuing authority, document number, document expiration date, document other information); level of national security clearance and expiration date; computer system user e-mail address; user access and permission rights, authentication certificates; digital signature information, and card holder unique identifier (CHUID).

Records maintained on card holders, entering VA facilities or using VA computer systems, are verified during the life cycle of audit records to include: Name, PIV Card serial number; date, time, and location of entry and exit; contractor company name (if applicable); level of national security clearance and expiration date; digital signature information; computer access dates, times, and locations.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; 38 U.S.C. 501; 40 U.S.C. 11331; 44 U.S.C 3544; Executive Order 9397; Homeland Security Presidential Directive 12; Federal Information Processing Standard 201–1.

PURPOSE:

The information collected in this system of records is used to a) ensure the safety and security of VA facilities, systems, or information, (b) verify that all persons entering Federal facilities, using Federal information resources, or accessing sensitive or classified information are authorized to do so; (c) track and control PIV cards issued to persons entering and exiting the facilities, using systems, or accessing sensitive or classified information, including patient records. This system of records applies to all VA Federal employment and contract positions, and may include VA employees, contractors, and affiliates to the extent their duties require access to VA Federal facilities and/or information systems.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PUROSES 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, 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) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of embarrassment or harm to the reputations of the record subjects, harm to economic or property interests, identity theft or fraud, or harm to the security, confidentiality, or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure is to agencies, entities, or persons whom VA determines are reasonably necessary to assist in or carry out the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

3. 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.

4. VA may disclose the 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.

5. 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.

6. VA may disclose the information to the Federal Labor Relations Authority (FLRA) 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.

7. 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.

8. 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.

9. VA may disclose information in this system of records to the Department of Justice (DOJ) and Office Personnel Management (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 DOJ's or OPM'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.

10. 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 in locked containers and electronically in secure locations.

RETRIEVABILITY:

Records may be retrieved by name of the individual, Cardholder Unique Identification (CHUID) Number, Social Security Number (SSN), and/or by any other unique individual identifier.

SAFEGUARDS:

Paper records are kept in locked cabinets in secure local VA facilities and access to them is restricted to individuals whose role requires use of the PIV records. Electronic records are kept in the PIV Identity Management System servers maintained at VA Data Centers in Falling Waters; WV, Hines, IL; and Austin Automation Data Center, Austin, TX. Access to the records is restricted to those with a specific role in the PIV process that requires access to PIV applicant data in order to perform their duties, and who have been given a PIV card for authentication, and a password to access the system of records. The computer servers in which records are stored are located in secure, monitored facilities.

Electronic records at the Data Centers 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.

A Privacy Act Warning Notice appears on the Web-based PIV Registration Portal screen when records containing information on individuals are first displayed. Data exchanged between the PIV servers located in VA data centers, and PC computer equipment at PIV registration offices are encrypted using SSL encryption (HTTPS) over commonly available Internet browsers. Backup tapes are stored in a locked and controlled room in a secure, off-site location.

An audit trail is maintained and reviewed periodically to identify unauthorized attempts to access, and actual unauthorized access. Persons given roles in the PIV process must complete training specific to their roles to ensure they are knowledgeable about how to protect individually-identified information.

RETENTION AND DISPOSAL:

Records relating to persons covered by this system are retained in accordance with General Records Schedule 18, Item 17. Unless retained for specific, ongoing security investigations, and in accordance with NARA, all of the PIV collected data will be retained for a minimum of 7.5 years beyond the term of employment, unless otherwise directed.

In accordance with HSPD–12, PIV Cards are deactivated within 18 hours from the notification time for cardholder separation, loss of card, or expiration. The information on PIV Cards is maintained in accordance with General Records Schedule 11, Item 4. PIV Cards are destroyed by shredding, typically within 90 days after deactivation.

SYSTEM MANAGER AND ADDRESS:

VA PIV Program Manager, Office of Human Resources (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 request in writing, signed, 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 above.

CONTESTING RECORD PROCEDURE:

Same as Notification procedures above. 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 PIV applicant (employee, contractor, or affiliate); the VA Active Directory; PIV applicant supervisor; existing VA personnel file; PIV-compliant identity documents; former sponsoring agency; other Federal agencies; contract employer; former employer.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. E8–6120 Filed 3–25–08; 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 of System of Records ''Health Care Provider Credentialing and Privileging Records—VA.''

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. The Department of Veterans Affairs (VA) is amending the system of records, known as ''Health Care Provider Credentialing and Privileging Records—VA'' (77VA10Q) as set forth in the **Federal Register** 55 FR 30790 dated 12/6/01. VA is amending the system notice by revising the paragraphs on System Location, Categories of Records in the System, Routine Uses, System Manager(s) and Address, and Record Source Categories. VA is republishing the system notice in its entirety at this time.

DATES: Comments on the amendment of this system of records must be received no later than April 25, 2008. If no public comment is received, the new system will become effective April 25, 2008.

ADDRESSES: Written comments may be submitted through *http://*