Privacy Impact Assessment - 2009 (Form) / Personal Identification Verification-2009 (Item)

PIA SECTIONS 1 - 4

Part I. Project Identification and Determination of PIA Requirement

1. PROJECT IDENTIFICATION:

1.1) Project Basic Information:

1.1.a) Project or Application Name:

Personal Identification Verification-2009

1.1.b) OMB Unique Project Identifier:

029-00-02-00-01-1034-00-404-140

1.1.c) Project Description

Project description is pre-populated from Exhibit 300 Part I.A.8. You will not be able to edit the description on this form.

Homeland Security Presidential Directive-12, "Policy for a Common Identification Standard for Federal Employees and Contractors" (HSPD-12) was issued on August 27, 2004. HSPD-12 directed a new Federal standard for secure and reliable identification to be issued by Federal agencies for their employees and contractors. The National Institute of Standards and Technology (NIST) published Federal Information Processing Standards Publication 201-Personal Identity Verification (PIV) of Federal Employees and Contractors (FIPS 201) on February 25, 2005. The VA PIV Program evolved from the Department of Veterans Affairs Authentication and Authorization Infrastructure Program (AAIP). One of the objective of AAIP was to establish an enterprise and standards-based authentication and authorization infrastructure framework that would support secure and seamless transmission of business transactions and information within VA and to VA business and operational partners, through the use of smart card technology and Public Key Infrastructure ((PKI)). After ther release of HSPD-12 and FIPS 201, a decision was made to replace AAIP with the VA PIV program.

The initial conceptual approach for the VA PIV System was to build upon the existing AAIP System by adding required functionality and services to achieve compliance with HSPD-12 and FIPS 201. An AAIP-PIV business and engineering gap-analysis was performed, the lessons learned from the AAIP effort were considered, and a Services Oriented Architecture (SOA) was established. The SOA approach defines the system in terms of Services, Components, and Objects. Each service within the VA PIV System is wrapped with web services and delivers services over well defined interfaces. The services required within the PIV solution include:
. Enrollment
. Identity and Access Management
. Security
. Data Support
. Publication
. Audit
. Archive
. Secure Data Storage
. Human Machine Interfaces
. Card Management
. Public Key Infrastructure

1.1.d) Additional Project Information (Optional)

The project description provided above should be a concise, stand-alone description of the project. Use this section to provide any important, supporting details.

Homeland Security Presidential Directive-12, "Policy for a Common Identification Standard for Federal Employees and Contractors" (HSPD-12) was issued on August 27, 2004. HSPD-12 directed a new Federal standard for secure and reliable identification to be issued by Federal agencies for their employees and contractors. The National Institute of Standards and Technology (NIST) published Federal Information Processing Standards Publication 201-Personal Identity Verification (PIV) of Federal Employees and Contractors (FIPS 201) on February 25, 2005. FIPS 201 and its associated Special Publications provide a detailed specification for Federal agencies and departments deploying personal identity verification (PIV) cards for their employees and contractors. The VA PIV Program established a fully functional and compliant VA Personal Identity Verification System (VA PIV System) responsible for the issuance and management of PIV Cards.

The VA PIV Program evolved from the Department of Veterans Affairs Authentication and Authorization Infrastructure Program (AAIP). One of the objectives of AAIP was to establish an enterprise and standards-based authentication and authorization infrastructure framework to support secure and seamless transmission of business transactions and

information within VA and t o VA business and operational partners, through the use of smart card technology and Public Key Infrastructure (PKI). After the release of HSPD-12 and FIPS 201, a decision was made to replace AAIP with the VA PIV program.

FIPS 201 consists of two parts. The first part defines specific roles and processes while the second part defines technical requirements. The VA PIV program implemented Part I of FIPS 201 between October 2005 and September 2006. The program disseminated guidance and implemented the FIPS 201 PIV card processes throughout the Department and achieved compliance with the Presidential mandate within the stipulated deadlines.

Implementation of Part II of FIPS 201 began in October of 2005. The initial conceptual approach for the VA PIV System was to build upon the existing AAIP System by adding required functionality and services to achieve compliance with HSPD-12 and FIPS 201. An AAIP-PI business and engineering gap-analysis was performed and it was determined that building upon the AAIP System was not feasible due to cost and schedule risks. The VA PIV Program considered the lessons learned from the AAIP effort and established a new engineering approach for the VA PIV System which embraced Services Oriented Architecture (SOA). The SOA approach leveraged web-services and standards based interfaces to accomplish four objectives:
. Utilize selected pieces of the AAIP solution to build a transitional PIV solution that is compliant with federal guidelines and the PIV II implementation date.
. Permit the build of an incremental solution that achieves compliance with HSPD-12 and FIPS 210 in phases.
. Allow for a decoupling of VA PIV System component integration and employ a model of supplier and consumer services consistent with industry best practices.
. Provide a means to leverage the services of the VA PIV System into an Enterprise vision of identity and access management, making the both solution forward-looking and Enterprise capable.
. Integrate PIV System services into an identity and access management solution that supports the needs of the VA Enterprise.

The change to an SOA approach allowed VA to "go live" with the transitional VA PIV System (Version 0.5) on October 27, 2006 and to meet the OMB implementation deadline. Version 0.5 provides the architectural baseline that will carry forward into subsequent phases of the program.

The VA PIV Program is currently implementing the second phase of implementation, with an expected delivery date of June 30, 2007. This phase of the system implementation provides the VA with the fully compliant PIV Solution, dubbed the VA PIV System version 1.0. The VA PIV System will incorporate elements in the production system that include the biometric services, the PIV Card stock, and the supporting workflow and digital signature processes that will provide the VA with a fully compliant PIV solution, as well as embrace the requirement of the Government Paperwork Elimination ACT. (GPEA) through the implementation of a fully electronic enrollment process. All transactions within the system that are required under FIPS 201-1 for enrollment of Card Applicants for PIV Cards will accomplished with electronic forms that apply PKI based digital signatures, thus eliminating the need for any paper forms within the deployed solution.

Certification and Accreditation: The program will certify and accredit the VA PIV System at a HIGH rating in accordance with VA direction and NIST SP 800-53 guidance.

1.2) Contact Information:

1.2.a) Person completing this document:	
Title:	Communication Lead
Organization:	Merlin International
Telephone Number:	202 274 9871
Email Address:	jennifer.smith7@va.gov
1.2.b) Project Manager:	
Title:	Brian Epley - VA PIV Project Manager
Organization:	Office of Information Technology
Telephone Number:	(202) 273-6240

Email Address:	brian.epley@va.med.gov
1.2.c) Staff Contact Person:	
Title:	IT Specialist
Organization:	Privacy Service (005P4)
Telephone Number:	202 357-3946
Email Address:	heidi.hamzi@va.gov

ADDITIONAL INFORMATION: If appropriate, provide explanation for limited answers, such as the development stage of project.

A privacy impact assessment (PIA) is required for all VA projects with IT system that collect, maintain, and/or disseminate personally identifiable information (PII) of the public, not including information of Federal employees and others performing work for VA (such as contractors, interns, volunteers, etc), unless it is a PIV project. All PIV projects collecting any PII must complete a PIA. PII is any representation of information that permits the identity of an individual to be reasonably inferred by either direct or indirect means. Direct references include: name, address, social security number, telephone number, email address, financial information, or other identifying number or code. Indirect references are any information by which an agency intends to identify specific individuals in conjunction with other data elements. Examples of indirect references include a combination of gender, race, birth date, geographic indicator and other descriptors.
2. a) Will the project collect and/or maintain personally identifiable information of the public in IT systems?
No.
2. b) Is this a PIV project collecting PII, including from Federal employees, contractors, and others performing work for VA?
Yes.

If "Yes" to either question then a PIA is required for this project. Complete the remaining question on this form. If "NO" to both questions then no PI is required for this project. Skip to section 13. and affirm.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section)
PIV information systems will only collect, maintain, and/or disseminate Personally Identifiable Information of Federal employees and others performing work for VA (such as contractors, interns, volunteers, etc.). Although the e-Gov Act of 2002 specifically requires PIAs for IT systems that collect, maintain, and /or disseminate Personally Identifiable Information of the public, it does not include information of Federal employees and others performing work for VA (such as contractors, interns, volunteers, etc). However, OMB specifically requires the completion of PIA to meet the privacy requirements of FIPS 201-1.

2. DETERMINATION OF PIA REQUIREMENTS:

A privacy impact assessment (PIA) is required for all VA projects with IT systems that collect, maintain, and/or disseminate personally identifiable information (PII) of the public, not including information of Federal employees and others performing work for VA (such as contractors, interns, volunteers, etc.), unless it is a PIV project. All PIV projects collecting any PII must complete a PIA. PII is any representation of information that permits the identity of an individual to be reasonably inferred by either direct or indirect means. Direct references include: name, address, social security number, telephone number, email address, financial information, or other identifying number or code. Indirect references are any information by which an agency intends to identify specific individuals in conjunction with other data elements. Examples of indirect references include a combination of gender, race, birth date, geographic indicator and other descriptors.

2.a) Will the project collect and/or maintain personally identifiable information of the public in IT systems?

No

2.b) Is this a PIV project collecting PII, including from Federal employees, contractors, and others performing work for VA?

Yes

If "YES" to either question then a PIA is required for this project. Complete the remaining questions on this form. If "NO" to both questions then no PIA is required for this project. Skip to section 14 and affirm.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

PIV information systems will only collect, maintain, and/or disseminate Personally Identifiable Information of Federal employees and others performing work for VA (such as contractors, interns, volunteers, etc.). Although the e-Gov Act of 2002 specifically requires PIAs for IT systems that collect, maintain, and/or disseminate Personally Identifiable

Information of the public, it does not include information of Federal employees and others performing work for VA (such as contractors, interns, volunteers, etc.), However, OMB specifically requires the completion of a PIA to meet the privacy requirements of FIPS 201-1.

Part II. Privacy Impact Assessment

3. PROJECT DESCRIPTION:

Enter the information requested to describe the project.

3.a) Provide a concise description of why personal information is maintained for this project, such as determining eligibility for benefits or providing patient care.

3. a) Provide a concise description of why personal information is maintained for this project, such as determining eligibility for benefits or providing patient care.
Personal information of employees, contractors, volunteers and affiliates will be collected and maintained from those requesting VA identification badges, in accordance with HSPD-12 mandate and related FIPS 201-1 privacy data collection requirements.
The goal of the PIV System is to achieve compliance with HSPD-12 and FIPS 201-1.

Within the context of this goal, the system intends to provide:

. Personal Identity Verification (PIV) cards based on secure and reliable forms of identification credentials.
. Issuance of PIV Credentials based on validation of an individual's true identity and validation of the organization affiliation.
. PIV credential holder Identity Management.
. Access Management and security policy enforcement surrounding the PIV processes.
. PIV Credential enrollment, registration, issuance and lifecycle management automation.

3.b) What specific legal authorities authorize this project, and the associated collection, use, and/or retention of personal information?

In accordance with HSPD-12 and FIPS 201-1, personal data such as fingerprints, personal information, and facial images will collected and stored for issuing PIV cards to federal employees and contractors, and for conducting PIV card lifecycle maintenance functions. The biographic and biometric information collected will be used to conduct a security threat assessment that includes a criminal history records check. The fingerprints will be used to verify identity of the holder of the credential and the photograph will be collected so that it can be printed on the PIV Card as a means to identify the cardholder. Biometric minutiae data will be deposited onto secure containers within the PIV Cards in accordance with the requirements from FIPS 201-1 and NIST SP 800-76. Any biometric information that is collected from the PIV solution will be immediately and securely purged from the system once the PIV Cards are manufactured and provided to the Card Applicants. The VA PIV System will not store biometric information that pertains to Card Applicants for any period of time longer than is required to manufacture a PIV Card, in order to minimize security exposure that is associated with storing privacy data. Further, any biometric information that is stored on the PIV Card is controlled and safeguarded by the actual smart card device, and the security boundaries that are associated with those tokens.

The risk assessments and technical solution provided by these PIV Card products has been fully assessed and/or tested by the NIST, FBI, GSA, and OMB, and they have been approved by those agencies as acceptable for Federal Government use. The VA will utilize the products that are published within the GSA Approved Product List (APL), which signifies that these devices are secure and provide only the necessary and approved interfaces to access privacy related data. Lastly, the personal information that pertains to a specific Card Applicant is secured by a full Role Based Access Control (RBAC) security model that is in place within the VA PIV System, and has been properly assessed and approved by the Office of Cyber and Information Security (OCIS) within the certification off accreditation process. This signifies the VA PIV System as a security system that has undergone rigorous assessment and testing, and that the environment provides the proper security controls to safeguard any personal information that is gathered herd for a Card Applicant

3.c) Identify, by selecting the appropriate range from the list below, the approximate number of individuals that (will) have their personal information stored in project systems.

100,000 - 999,999

3.d) Identify what stage the project/system is in: (1) Design/Planning, (2) Development/Implementation, (3) Operation/Maintenance, (4) Disposal, or (5) Mixed Stages.

(2) Development/Implementation

3.e) Identify either the approximate date (MM/YYYY) the project/system will be operational (if in the design or development stage), or the approximate number of years that the project/system has been in operation.

0.5 years (first implementation occurred 10/27/2006); fully PIV-compliant cards will be issued beginning 6/30/2007.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

4. SYSTEM OF RECORDS:

The Privacy Act of 1974 (Section 552a of Title 5 of the United States Code) and VA policy provide privacy protections for employee or customer information that VA or its suppliers maintain in a System of Records (SOR). A SOR is a file or application from which personal information is retrieved by an identifier (e.g. name, unique number or symbol). Data maintained in a SOR must be managed in accordance with the requirements of the Privacy Act and the specific provisions of the applicable SOR Notice. Each SOR Notice is to be published in the Federal Register. See VA Handbook 6300.5 "Procedures for Establishing & Managing Privacy Act Systems Of Records", for additional information regarding Systems of Records.

4.a) Will the project or application retrieve personal information on the basis of name, unique number, symbol, or other identifier assigned to the individual?

If "No" then skip to section 5, 'Data Collection'.

Yes

4.b) Are the project and/or system data maintained under one or more approved System(s) of Records?

IF "No" then SKIP to question 4.c.

No

4.b.1) For each applicable System of Records, list:

(1) The System of Records identifier (number),

103VA07B

(2) The name of the System of Records, and

Police and Security Records 4B12

(3) Provide the location where the specific applicable System of Records Notice(s) may be accessed (include the URL).

http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2002/pdf/02-31709.pdf

IMPORTANT: For each applicable System of Records Notice that is not accessible via a URL: (1) Provide a concise explanation of why the System of Records Notice is not accessible via a URL in the "Additional Information" field at the end of this section, and (2) Send a copy of the System of Records Notice(s) to the Privacy Service.

4.b.2) Have you read, and will the application comply with, all data management practices in the System of Records Notice(s)?

Yes

4.b.3) Was the System(s) of Records created specifically for this project, or created for another project or system?

Created for another project or system

If created for another project or system, briefly identify the other project or system.

It was created for a variety of S&LE functions, to include ID badging.

4.b.4) Does the System of Records Notice require modification?

If "No" then skip to section 5, 'Data Collection'.

Modification of the System of Records is Required

4.b.5) Describe the required modifications.

The SORN does not currently cover the collection of fingerprints. Fingerprints are not currently collected or stored by the VA PIV System, but will be part of future System versions. The storage of biometric information is only for very short periods of time, and the VA PIV System does not and will not continuously grow a repository of biometric information. The data is securely wiped from the System once the PIV Card has been properly manufactured and accepted by the Card Applicant.

To address the PIV processes, the new SORNs are being developed (are currently in the VA approval process) for or PIV:

1. The Identity Management SORN, which covers the PIV Maintenance function
2. The Personnel Security System SORN, which includes the fingerprints and other personal security information.

4.c) If the project and/or system data are not maintained under one or more approved System(s) of Records, select one of the following and provide a concise explanation.

Not Applicable

Explanation:

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

PIA SECTION 5

Project Name

Personal Identification Verification-2009

5. DATA COLLECTION:

5.1 Data Types and Data Uses

Identify the types of personal information collected and the intended use(s) of that data:

a) Select all applicable data types below. If the provided data types do not adequately describe a specific data collection, select the "Other Personal Information" field and provide a description of the information.

b) For each selected data type, concisely describe how that data will be used.

Important Note: Please be specific. If different data types or data groups will be used for different purposes or multiple purposes, specify. For example: "Name and address information will be used to communicate with individuals about their benefits, while Name, Service, and Dependent's information will be used to determine which benefits individuals will be eligible to receive. Email address will be used to inform individuals about new services as they become available."

Yes	**Veteran's or Primary Subject's Personal Contact Information (name, address, telephone, etc.)**

Specifically identify the personal information collected, and describe the intended use of the information.

Personal contact, biometric, and biographic information for applicants of a PIV credential (VA identification badge), such as employees, contractors, volunteers and other affiliates will be collected.

Veterans who are not VA employees, contractors, volunteers or other affiliate will NOT have their personal information in the PIV information system . The purpose of collecting this information is to issue a PIV badge to an authorized individual. The biographic and biometric information collected will be used to conduct a security threat assessment that includes a criminal history record check. The fingerprints will used to verify identity of the holder of the credential and the photograph will be collected so that it can be printed o the PIV Card as a means to identify the cardholder.

Intended use of the data is to identify and validate an employees biographic data in order to issue them a valid government PIV card which contains pertinent applicant data required by FIPS 201-1, such as name, agency, photo image, etc.

Other than information to be printed on the actual PIV card, PIV credential applicants may be required to submit additional personal information - outside of the PIV enrollment process-regarding their personal background/employment history as part of the employment application process. "The forms used fo this detailed below in the Collection Media Section. The information collected is standard across all government agencies and is used solely for the purpose of conducting background investigations, and is identified on the fields of the VA0711 form.

Applicant Information:
. Name of Applicant
. DOB
. SSN
. Name & Address of Facility or assigned duty station
. Name of Sponsoring Dept.
. Type of Request
. Type of Badge
. Type of Access
. Employment Status
. Employment expiration date
. Name of firm (contractor)
. Contract Number (contractor)

. Contract expiration date (contractor)
. Name of COTR (contractor)
. Name of responsible VA organization and mail routing symbol
. Date signed by sponsor
. Work phone of sponsor
. Type of BI
. Date initiated BI
. Date adjudicated BI
. Name of sponsor
. Date signed
. Applicants request for One VA Identification Card
. Facial image (photos)
. Fingerprints (although they are currently collected outside of PIV)

Yes	**Other Personal Information of the Veteran or Primary Subject**

Specifically identify the personal information collected, and describe the intended use of the information.

Personal email, home phone number, for the purposes of contacting the applicant outside of the office environment.

No	**Dependent Information**

Specifically identify the personal information collected, and describe the intended use of the information.

No

No	**Service Information**

Specifically identify the personal information collected, and describe the intended use of the information.

No	**Medical Information**

Specifically identify the personal information collected, and describe the intended use of the information.

No	**Criminal Record Information**

Specifically identify the personal information collected, and describe the intended use of the information.

Criminal Record Information will not be collected b the VA PIV System.

No	**Guardian Information**

Specifically identify the personal information collected, and describe the intended use of the information.

No	**Education Information**

Specifically identify the personal information collected, and describe the intended use of the information.

No	**Rehabilitation Information**

Specifically identify the personal information collected, and describe the intended use of the information.

Yes	**Other Personal Information (specify):**

The "Other Personal Information" field is intended to allow identification of collected personal information that does not fit the provided categories. If personal information is collected that does not fit one of the provided categories, specifically identify this information and describe the intended use of the information.

Yes, see the information above.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

5.2 Data Sources

Identify the source(s) of the collected information.

a) Select all applicable data source categories provided below.

b) For each category selected:

i) Specifically identify the source(s) - identify each specific organization, agency or other entity that is a source of personal information. ii) Provide a concise description of why information is collected from that source(s). iii) Provide any required additional clarifying information.

Your responses should clearly identify each source of personal information, and explain why information is obtained from each identified source. (Important Note: This section addresses sources of personal information; Section 6.1, "User Access and Data Sharing" addresses sharing of collected personal information.)

Note: PIV projects should use the "Other Source(s)" data source.

No	**Veteran Source**

Provide a concise description of why information is collected from Veterans. Provide any required additional, clarifying information.

No	**Public Source(s)**

i) Specifically identify the Public Source(s) - identify the specific organization(s) or other entity(ies) that supply personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.

No	**VA Files and Databases**

i) Specifically identify each VA File and/or Database that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.

Yes	**Other Federal Agency Source(s)**

i) Specifically identify each Federal Agency that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.

Within the PIV process, Sponsors will submit fingerprint information to OPM using the OPM provided tools (e.g., the EQIP system) to perform a Special Agency Check (SAC) as part of the hiring process. The results of this check are to be provided to the Security Investigation Center (SIC) in Arkansas, which is accessed by the PIPS portal interface, also provided by OPM. The PIV process has a dependency form that out-of- band process for successfully adjudicate ad SAC, prior to issuing a PIV Card to a Card Applicant. the VA PIV System does not receive any personal information with this external and out of band process, but relies upon the result s of that process as a trigger to allowing or disallowing a PIV Card t o be issued.

Under certain circumstances when a federal employee transfers from another agency, evidence of a background investigation etc. could be supplied by a former agency to the SIC.

No	**State Agency Source(s)**

i) Specifically identify each State Agency that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.

No	**Local Agency Source(s)**

i) Specifically identify each Local Agency (Government agency other than a Federal or State agency) that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.

Yes	**Other Source(s)**

i) If the provided Data Source categories do not adequately describe a source of personal information, specifically identify and describe each additional source of personal information. ii) For each identified data source, provide a concise description of why information is collected from that source. iii) Provide any required additional, clarifying information.

VA employees, contractors and affiliates, via the VA 0711 form, for t he purposes of issuing an ID badge.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

5.3 Collection Methods

Identify and describe how personal information is collected:

a) Select all applicable collection methods below. If the provided collection methods do not adequately describe a specific data collection, select the "Other Collection Method" field and provide a description of the collection method. b) For each collection method selected, briefly describe the collection method, and provide additional information as indicated.

Yes	**Web Forms:**	Information collected on Web Forms and sent electronically over the Internet to project systems.

Identify the URL(s) of each Web site(s) from which information will be submitted, and the URL(s) of the associated privacy statement. (Note: This question only applies to Web forms that are submitted online. Forms that are accessed online, printed and then mailed or faxed are considered "Paper Forms.")

The PIV enrollment process employs a Web-based enrollment portal that supports secure session connectivity (e.g., SSL v3.0/TLS v1.0) to infrastructure that is located in VA Data Centers. The infrastructure consists of web server platforms that are secure, certified and accredited and operated in physically secure environments at the data center locations. The portal is located on the VA Intranet at http://vaww.piv.va.gov/idm/piv.

Yes	**Paper Forms:**	Information collected on Paper Forms and submitted personally, submitted via Postal Mail and/or submitted via Fax Machine.

Identify and/or describe the paper forms by which data is collected. If applicable, identify standard VA forms by form number.

Information specific to the request for a PIV card is collected on VA Form 0711 for the manual processes that are supported under FIPS 201-1 Part 1. The electronic process employs electronic forms that apply PKI based digital signatures and no paper forms are involved in that process.

No	**Electronic File**	Information stored on one computer/system (not entered via a Web Form) and

	Transfer:	transferred electronically to project IT systems.

Describe the Electronic File Transfers used to collect information into project systems. (Note: This section addresses only data collection – how information stored in project systems is acquired. Sharing of information stored in project systems and data backups are addressed in subsequent sections.)

Authoritative and approved sources within the VA will need to send electronic fingerprint information to OPM using the EQIP tool. The VA PIV Registrar role is an approved source that can submit fingerprints using available tools conected to EQIP, but these processes are not integrated with the VA PIV System and the System does not store any of these transactions. They are performed separate and apart from the VA PIV System as an out of band process.

Yes	**Computer Transfer Device:**	Information that is entered and/or stored on one computer/ system and then transferred to project IT systems via an object
		or device that is used to store data, such as a CD-ROM, floppy disk or tape.

Describe the type of computer transfer device, and the process used to collect information.

Offsite backup storage tapes are managed by data centers for securely storing collected privacy data in the same fashion that Veterans' privacy data are stored offsite for backup purposes.

No	**Telephone Contact:**	Information is collected via telephone.

Describe the process through which information is collected via telephone contacts.

Yes	**Other Collection Method:**	Information is collected through a method other that those listed above.

If the provided collection method categories do not adequately describe a specific data collection, select the "Other Collection Method" field and specifically identify and describe the process used to collect information.

Form SF 87: Fingerprints are taken electronically on the PIV enrollment fingerprinting machine. The fingerprinting machine will transmit an electronic copy in EFTS format of the fingerprints to OPM/FBI through a secure network connection. Copies of fingerprints are maintained locally in temporary cache memory until they are processed into EFTS format and transmitted t o OPM/FBI. They are then discarded at the VA PIV enrollment site without being stored.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

5.4 Notice

The Privacy Act of 1974 and VA policy requires that certain disclosures be made to data subjects when information in identifiable form is collected from them. The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

5.4.a) Is personally identifiable information collected directly from individual members of the public and maintained in the project's IT systems?

No

Note: If you have selected NO above, then SKIP to Section 5.5, 'Consent'.

5.4.b) Is the data collection mandatory or voluntary?

Mandatory

5.4.c) How are the individuals involved in the information collection notified of the Privacy Policy and whether provision of the information is mandatory or voluntary?

Applicants are requested to read and sign a Privacy Impact Statement during enrollment and at card issuance stating they understand the impact of the PIV card issuance and usage of the card and their privacy data. The PIV training process for PIV deployment will also provide user training regarding the use of privacy data.

5.4.d) Is the data collection new or ongoing?

Ongoing

5.4.e.1) If personally identifiable information is collected online, is a privacy notice provided that includes the following elements? (Select all applicable boxes.)

	Not applicable
	Privacy notice is provided on each page of the application.
Yes	**A link to the VA Website Privacy Policy is provided.**
Yes	**Proximity and Timing: the notice is provided at the time and point of data collection.**
Yes	**Purpose: notice describes the principal purpose(s) for which the information will be used.**
Yes	**Authority: notice specifies the legal authority that allows the information to be collected.**
Yes	**Conditions: notice specifies if providing information is voluntary, and effects, if any, of not providing it.**
Yes	**Disclosures: notice specifies routine use(s) that may be made of the information.**

5.4.e.2) If necessary, provide an explanation on privacy notices for your project:

The PIV Privacy Impact Statement is included in VA Form 0711 and on the VA PIV System Enrollment Portal.

5.4.f) For each type of collection method used (identified in Section 5.3, "Collection Method"), explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

Note: if PII is transferred from other projects, explain any agreements or understandings regarding notification of subjects.

Yes	**Web Forms:**

Explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

The PIV process employs a Web-base electronic enrollment form. The applicant will be informed of the purpose of the collected data, how it will be used to create a PIV card, legal authority for doing so, and other uses of the collected data. In addition, the applicant signature page will identify they have read the privacy implications of the collected personal data, and understand the implications and purpose of the data.

Yes	**Paper Forms:**

Explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

The 0711 paper form will also be used in the early stages of the PIV enrollment process until digital signatures are built into the electronic enrollment process. In the Privacy Notice included as part of the 0711 form, the Applicants will be informed of the purpose of the collected data, how it will be used to create a PIV card, legal authority for doing so, and other uses of the collected data. In addition, the applicant signature page will identify they have read the privacy implications of the collected personal data, and understand the implications and purpose of the data.

No	**Electronic File Transfer:**

For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to notify subjects regarding:

a) What they will be told about the information collection? b) How the message will be conveyed (e.g. written notice, electronic notice if web-based collection, etc.)? c)How a privacy notice is provided?

Yes	**Computer Transfer Device:**

For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to notify subjects regarding:

a) What they will be told about the information collection? b) How the message will be conveyed (e.g. written notice, electronic notice if web-based collection, etc.)? c)How a privacy notice is provided?

Information via this method is for backup purposes only - information is not collected from subjects via Computer Transfer Device.

No	**Telephone:**

Explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

Yes	**Other Method:**

Explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

5.5 Consent For Secondary Use of PII:

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

5.5.a) Will personally identifiable information be used for any secondary purpose?

Note: If you have selected No above, then SKIP to question 5.6, "Data Quality."

No

5.5.b) Describe and justify any secondary uses of personal information.

5.5.c) For each collection method identified in question 5.3, "Collection Method," describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.

Some examples of consent methods are: (1) Approved OMB consent forms and (2) VA Consent Form (VA Form 1010EZ). Provide justification if no method of consent is provided.

	Web Forms:

Describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.

	Paper Forms:

Describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.

	Electronic File Transfer:

For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to provide the following:

a) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. b) The opportunities individuals have to grant consent for particular uses of the information. c) How individuals may grant consent.

	Computer Transfer Device:

For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to provide the following:

a) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. b) The opportunities individuals have to grant consent for particular uses of the information. c) How individuals may grant consent.

	Telephone Contact Media:

Describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.

	Other Media

Describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

5.6 Data Quality

5.6.a) Explain how collected data are limited to required elements:

The PIV enrollment form is Web-based and/or paper-based (through VA Form 0711). The standardized form has been approved by the VA for vetting a candidate PIV applicant. The Web-based portal data collection fields cannot be modified, added, or omitted during the PIV applicant enrollment procedures. In addition, all required fields must be completed in order for the enrollment process to be approved for the next steps leading to card issuance. The data collected from the Web-based enrollment process leads to card issuance data provisioning.
The VA 0711 paper form data collection is to provide a digital signature corresponding to acknowledgement of both the paper-and web-based enrollment forms. The form has been approved by OMB, which examines the information collected and the intended purpose.

5.6.b) How is data checked for completeness?

The electronic Web-based portal of the VA PIV System will not allow a record to be entered and saved electronically by an individual unless all required fields are complete; a PIV card cannot be issued with an incomplete system record.

In order to enforce the completeness of collected data, the Enrollment Service integrates with the Security and IAM Services to receive security services and control services that manage its operation. It further implements some control and security services of its own as it pertains to the full entry of data and submission of information to the VA PIV System. Enrollment services are provided via the We-based portal interface to the authoritative and administrative PIV roles.

5.6.c) What steps or procedures are taken to ensure the data are current and not out of date?

All PIV personnel records are considered current and up-to-date as long as the badge has not expired. Employees, contractors, volunteers and affiliates are required to update changes to their information in the event of name changes, address, etc. There are clearance procedures for employees leaving VA to ensure they are removed from systems. Contractors are also required as part of their contracts to return issued badges when expired or at the end of the contract of ensure they are removed form the system . Both dates are accommodated in the PIV system with the revocation of the contractor certificates active on the card which grant them logical and/or physical access privileges until termination. Managers of volunteers are required to collect badges upon conclusion of work and return them to the Issuer.

5.6.d) How is new data verified for relevance, authenticity and accuracy?

The Sponsor, Registrar, and Applicant will will verify new Applicant data sum bitted during PIV card lifecycle operations and maintenance functions, such as card renewal, charge in marital status, etc, using approved I-9 documents, and by signing (either on paper or electronic VA 0711 forms) the new data input, thereby approving the accuracy.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

PIA SECTIONS 6 - 13

Project Name

Personal Identification Verification-2009

6. Use and Disclosure

6.1 User Access and Data Sharing

Identify the individuals and organizations that have access to system data.

--> Individuals - Access granted to individuals should be limited to the data needed to perform their assigned duties. Individuals with access to personal information stored in project system must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to prevent as well as detect unauthorized access and browsing.

--> Other Agencies – Any Federal, State or local agencies that have authorized access to collected personal information must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to protect personal information.

--> Other Systems – Information systems of other programs or projects that interface with the information system(s) of this project must be identified and the transferred data must be defined. Also, the controls that are in place to ensure that only the defined data are transmitted must be defined.

6.1.a) Identify all individuals and organizations that will have access to collected information. Select all applicable items below.

Yes	**System Users**

Yes	**System Owner, Project Manager**

Yes	**System Administrator**

Yes	**Contractor**

If contractors to VA have access to the system, describe their role and the extent of access that is granted to them. Also, identify the contract(s) that they operate under.

For the initial PIV deployment, VA contractors on the PIV contract who designed and integrated the PIV system into the VA enterprise will perform Tier III maintenance operations and general administrative operations to the PIV system. Specifically, contractors supporting the deployment of the solution to the field will have access to the system to perform administrative operations and maintenance/set up operations. Designated contractors supporting the solution in VA Data Centers will perform administrative operations and maintenance operations. PIV contracts include: PIV Systems Compliance Integration and Implementation Services and Implementation and Training Support for the PIV Program (Formerly known as the Authentication and Authorization Infrastructure Project).

No	**Internal Sharing: Veteran Organization**

If information is shared internally, with other VA organizations identify the organization(s). For each organization, identify the information that is shared and for what purpose.

No	**Other Veteran Organization**

If information is shared with a Veteran organization other than VA, identify the organization(s). For each organization, identify the information that is shared and for what purpose.

Yes	**Other Federal Government Agency**

If information is shared with another Federal government agency(ies), identify the agency(ies). For each organization, identify the information that is shared and for what purpose.

OPM and FBI will be reviewing PIV applicant fingerprint data for comparison against theri database and return the results.

No	**State Government Agency**

If information is shared with a State government agency(ies), identify the agency(ies). For each organization, identify the information that is shared and for what purpose.

No	**Local Government Agency**

If information is shared with a local government agency(ies), identify the agency(ies). For each organization, identify the information that is shared and for what purpose.

No	**Other Project / System**

If information is shared with other projects or systems:

1) Identify the other projects and/or systems, and briefly describe the data sharing. 2) For each project and/or system with which information will be shared, identify the information that will be shared with that project or system. 3) For each project and/or system with which information will be shared, describe why information is shared. 4) For each project and/or system with which information will be shared, describe who will be responsible for protecting the privacy rights of the individuals whose data will be shared across this interface.

No	**Other User(s)**

If information is shared with persons or organization(s) that are not described by the categories provided, use this field to identify and describe what other persons or organization(s) have access to personal information stored on project systems. Also, briefly describe the data sharing.

6.1.a.1) Describe here who has access to personal information maintained in project's IT systems:

Local issuance site Registrars will manage the secure storage of data captured on the hard-copy VA 0711 forms. they also have access to the same information stored at Data Centers on the PIV Web-based electronic enrollment forms. Only the Registrar, Issuers, Sponsors (for reviewing their data input), system administrators, and Tier III maintenance operations have access to the data maintained in the PIV system.

6.1.b) How is access to the data determined?

The Security Service of the VA PIV System is a critical component that protects sensitive, privacy, and agency-restricted data. this Service provides the compliance mechanism for the Federal Information Security Management Act 2002 (FISMA) and provides the assurance that the data collected, used and stored by the system is protected at an appropriate level to r restrict unauthorized access to sensitive information.

Access to the VA PIV System is controlled through a combination of Role Based Access Control (RBAC) and M of N access control services to data. The RBAC services are provided by the PIV Identity Access Management (IAM) Service, and consist of defined administrative roles that are permitted access on a component-per-component basis. The Security Service is established through the separation of the applications (e.g., Access Management Server), polices (e.g., Policy Store), and RBAC components (e.g., Access Management Server). By establishing this separation of function, the IAM Service has an architecture that does not lend itself to any one component being capable of accessing secure or sensitive data when compromised. Each of the three components of the Security Substructure must be valid and available to provide access to data. Additionally the RBAC model for access control provides a strong "least privilege" method that ensures no single individual can circumvent security controls to initiate changes or modification to system operation.

This access control system ensures that no single entity can perform configuration or modification of the system without conducting acts of collusion with other roles and entities. The M of N controls constitute a satisfaction mechanism to enforce separation of duty requirements for select components of the system.

Accounts are centrally managed by the IAM Service. Accounts are applied under strong audit and audit logs are digitally signed to detect modification and protect the integrity of the system. All audit materials are centralized in the Audit Server component within the IAM Service. Audit logs are protected over encrypted Web services and are securely deposited into the consolidated audit service.

Information flow within the VA PIV System is permitted based upon successful matching of identity, access rights validation, and funcnntion privilege. An entity must be strongly authenticated to provide assurance of the identity of the operator prior to granting access to a function. An authenticated entity must have approved access rights and the requested function must be appropriate for the role the individual/entity fills to successfully access a requested functionality.

Client services are provided with a session lock and session termination security control that is enforced by the PIV Card. After a specific number of incorrect attempts to access the PIV Card, the device will suspend its operation and require administrative intervention to unlock. This lock mechanism mitigates the risk of a brute-force attack to obtain access to privacy and personal data that is stored on the card.

6.1.c) Are criteria, procedures, controls, and responsibilities regarding access documented? If so, identify the documents.

Yes, the criteria, procedures, and responsibilities regarding access are documented in the VA PIV system Design Document.

In addition, an Operations and Maintenance manual will be provided to Operations personnel at the Data Centers, and an Enrollment Handbook and User Guide will be provided to the PIV administrators documenting access control rights and procedures.

6.1.d) Will users have access to all data on the project systems or will user access be restricted? Explain.

Information flow within the VA PIV system is permitted based upon successful matching of identity, access rights validation and function privilege. A user, or entity, must be strongly authenticated to provide assurance of the identity of the operator prior to granting access to a function. An authenticated entity must have approved access rights and the requested function must be a appropriate for the role the individual/entity fills to successfully access a requested functionality. Accordingly, only users having inherent assigned rights to access will be provided access by the system security controls.

6.1.e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by those having access? (Please list processes and training materials that specifically relate to unauthorized browsing)

Access to the VA PIV System is controlled through a combination of Role Based Access Control (RBAC) and M of N access control services. M of N security controls are in place to secure the generation of asymmetric key material used within the

Certificate Authority. The M of N controls offer split knowledge or split key services that require multiple operators to work together to obtain access to sensitive computing components of the VA PIV System. This access control ensures that no single entity can perform configuration or modification of the system without conducting acts of collusion with other roles and entities. The M of N controls constitute a satisfaction mechanism to enforce separation of duty requirements for select components of the system.

Accounts are centrally managed by the IAM Service. Accounts are applied under strong audit and audit logs are digitally signed to detect modification and protect the integrity of the system. All audit materials are centralized in the Audit Server component within the IAM Service. These materials include the logs of the PKI and CMS environments that are provided across the Shared Service Provided interface. Audit logs are protected over encrypted Web services and are securely deposited into the consolidated audit service.

6.1.f) Is personal information shared (is access provided to anyone other than the system users, system owner, Project Manager, System Administrator)? (Yes/No)

No

Note: If you have selected No above, then SKIP to question 6.2, "Access to Records and Requests for Corrections".

6.1.g) Identify the measures taken to protect the privacy rights of the individuals whose data will be shared.

The PIV privacy data collected is not shared with externally entities. However, regarding fingerprints collected during PIV enrollment for the purposes of adjudicating criminal background checks for PIV card applicants, OMP and FBI are responsible for protecting the privacy rights of the individuals for fingerprints that are recieved at their external sites. In addition, the VA does not store the captured fingerprints locally. In a future phase of the PIV effort, the fingerprint collection process will be integrated within the PIV registration process and transmitted to the FBI via the ETF standard. A SORN addressing the secure storage of fingerprint images and other security-related personnel information is in the process of being approved.

The VA has a secure FIPS 140-2 encrypted network connection for data transmission between OPM and FBI to mitigate any risk of data interception or modification. Accordingly, in the future PIV versions, the Registrar at the VA sites is responsible for protecting the privacy rights while collecting the fingerprints, during transmission and prior to OPM receiving ther fingerprints electronically or in paper form.

6.1.h) Identify who is responsible, once personal information leaves your project's IT system(s), for ensuring that the information is protected.

OPM a and FBI are responsible for protecting the privacy rights of the individuals for fingerprints that are received and stored at their external sites. They have been managing this fingerprint data from state and federal agencies for many years and have their federal security-approved controls in place.

6.1.i) Describe how personal information that is shared is transmitted or disclosed.

The VA has a secure FIPS 140-2 encrypted VPN network connection for fingerprint data transmission between OPM and FBI to mitigate any risk of data interception or modification.

6.1.j) Is a Memorandum of Understanding (MOU), contract, or any other agreement in place with all external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared? If an MOU is not in place, is the sharing covered by a routine use in the System of Records Notice? If not, explain the steps being taken to address this omission.

A System of Records Notice is in place with OPM as fingerprint data is collected and transmitted between VA and OPM for current VA badges.

6.1.k) How is the shared information secured by the recipient?

PIV-collected fingerprint data information is not currently saved or stored by VA. However, the same IAM security controls used for PIV applicant biographic privacy data are also employed for adjudication response information received from either OPM or FBI. OPM or FBI has their own federally approved policy controls in place for securing shared fingerprint information received from outside agencies.

6.1.l) What type of training is required for users from agencies outside VA prior to receiving access to the information?

None. These fingerprint data transmissions are normal ongoing daily operations at OPM and FBI.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

6.2 Access to Records and Requests for Corrections

The Privacy Act and VA policy provide certain rights and mechanisms by which individuals may request access to and amendment of information relating to them that is retained in a System of Records.

6.2.a) How can individuals view instructions for accessing or amending data related to them that is maintained by VA? (Select all applicable options below.)

	The application will provide a link that leads to their information.
	The application will provide, via link or where data is collected, written instructions on how to access/amend their information.
	The application will provide a phone number of a VA representative who will provide instructions.
Yes	**The application will use other method (explain below).**
	The application is exempt from needing to provide access.

6.2.b) What are the procedures that allow individuals to gain access to their own information?

Only during initial PIV enrollment are applicants permitted to view their current privacy data, and in the presence of the PIV Sponsor, they may amend or update the current PIV card enrollment information. Once the Applicant data is verified as accurate, the PIV enrollment steps will proceed for the PIV card to be issued, as long as the remaining enrollment and identity proofing requirements are met.

6.2.c) What are the procedures for correcting erroneous information?

See 6.2b

6.2.d) If no redress is provided, are alternatives available?

N/A

6.2.e) Provide here any additional explanation; if exempt, explain why the application is exempt from providing access and amendment.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

7 Retention and Disposal

By completing this section, you provide documented assurance that proper data retention and disposal practices are in place.

The "Retention and disposal" section of the applicable System of Records Notice(s) often provides appropriate and sufficiently detailed documented data retention and disposal practices specific to your project.

VA HBK 6300.1 Records Management Procedures explains the Records Control Schedule procedures.
System of Records Notices may be accessed via:
http://vaww.vhaco.va.gov//privacy/SystemofRecords.htm
or
http://vaww.va.gov/foia/err/enhanced/privacy_act/privacy_act.html
For VHA projects, VHA Handbook 1907.1 (Section 6j) and VHA Records Control Schedule 10-1 provide more general guidance.
VHA Handbook 1907.1 may be accessed at:
http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=434

For VBA projects, Records Control Schedule (RCS) VB-1 provides more general guidance. VBA Records Control Schedule (RCS) VB-1 may be accessed via the URL listed below.
Start by looking at the http://www.warms.vba.va.gov/20rcs.html

7.a) What is the data retention period? Given the purpose of retaining the information, explain why the information is needed for the indicated period.

In accordance with U.S. National Archives and Records Administration (NARA), all PIV-collected data will be retained for a minimum of 7.5 eyars beyond the term of employment, unless otherwise directed. However, the data retention period for the VA 0711 form is 10.5 years.

7.b) What are the procedures for eliminating data at the end of the retention period?

The IAM Service tracks all data elements within the system and has the ability to tag data that is no longer required in production/operation. these data elements and associated user profile packages are to be archived in accordance with NARA regulations and will be securely provided over the Web services (e.g., HTTPS) to an archive instance that is to be identified by the VA.

7.c) Where are procedures documented?

VA PIV System Design Document and the VA PIV Operations and Maintenance Procedures.

7.d) How are data retention procedures enforced?

PIV Data: The VA PIV system provides automated reminders in the Audit Sub-system. It is tied to the Security Service to eliminate any data retention/elimination errors.

Fingerprinting System: The system provides automated procedures for data elimination as soon as the data is sent to either OPM or DOJ.

7.e) If applicable, has the retention schedule been approved by the National Archives and Records Administration (NARA)?

Yes

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

PIV is following the NARA guidelines and VA document policies.

8 SECURITY

OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, (OMB M-03-22) specifies that privacy impact assessments must address how collected information will be secured.

8.1 General Security Measures

8.1.a) Per OMB guidance, citing requirements of the Federal Information Security Management Act, address the following items (select all applicable boxes.):

Yes	The project is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured.
Yes	The project has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.
Yes	Security monitoring, testing, and evaluating are conducted on a regular basis to ensure that controls continue to work properly, safeguarding the information.

8.1.b) Describe the security monitoring, testing, and evaluating that is conducted on a regular basis:

The Security Service of the VA PIV System is a critical component that protects sensitive, privacy, and agency restricted data. This service provides the compliance mechanism for the Federal Information Security Management Act of 2002

(FISMA) and provides the assurance that the data collected and used and store by the system is protected at an appropriate level to restrict unauthorized access to sensitive information. Accounts are centrally managed by the IAM Service.

User Accounts are applied under strong audit and audit logs are digitally signed to detect modification and protect the integrity of the system. All audit materials are centralized in the Audit Server component within the IAM Service. These materials include the logs of PKI and CMS environments that are provided across the Shared Service Provider interface. Audit logs are protected over encrypted. Web services and are securely deposited into the consolidated audit service.

8.1.c) Is adequate physical security in place to protect against unauthorized access?

Yes

8.2 Project-Specific Security Measures

8.2.a) Provide a specific description of how collected information will be secured.

• A concise description of how data will be protected against unauthorized access, unauthorized modification, and how the availability of the system will be protected.

• A concise description of the administrative controls (Security Plans, Rules of Behavior, Procedures for establishing user accounts, etc.).

• A concise description of the technical controls (Access Controls, Intrusion Detection, etc.) that will be in place to safeguard the information.

• Describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses. For example, are audit logs regularly reviewed to ensure appropriate use of information? Are strict disciplinary programs in place if an individual is found to be inappropriately using the information?

Note: Administrative and technical safeguards must be specific to the system covered by the PIA, rather than an overall description of how the VA's network is secured. Does the project/system have its own security controls, independent of the VA network? Is so, describe these controls.

The Security Service of VA PIV System is a critical component that protect sensitive, privacy and agency restricted data. This Service provides the compliance mechanism fro the Federal Information Security Management Act of 2002 (FISMA) and provides the assurance that the data collected, used and stored by the system is protected at an appropriate level to restrict unauthorized access to sensitive information.

Access to the VA PIV System is controlled through a combination of Role Based Access Control (RBAC) and M of N access control services. The RBAC services are provided by the IAM Service, and consist of defined administrative roles that are permitted access on a component per component basis. The Security Service is established through the separation of the applications (e.g., Access Management Server), policies (e.g., Policy Store), and RBAC components (e.g., Access Management Serer). By establishing this separation of function, the IAM Service has an architecture that does not lend itself to any one component being capable of accessing secure or sensitive data when compromised. Each of the three components of the Security Substructure must be valid and available to provide access to data. Additionally the RBAC model for access control provides a strong "least privilege" method that ensures no single individual can circumvent security controls to initiate changes or modification to system operation.

M of N security controls are in place to secure the generation of asymmetric key material used within the Certificate Authority. The M of N controls offer split knowledge or split key services that require multiple operators to work together to obtain access to sensitive computing components of the VA PIV System. This access control ensures that no single entity can perform configuration or modification of the system without conducting acts of collusion with other roles and entities. The M of N controls constitute a satisfaction mechanism to enforce separation of duty requirements for select components of the system.

Accounts are centrally managed by the IAM Service. Accounts are applied under strong audit and audit logs are digitally signed to detect modification and protect the integrity of the system. All audit materials are centralized in the Audit Server component within the IAM Service. These materials include the logs of the PKI and CMS environment that are provided across the Shared Service Provider interface. Audit logs are protected over encrypted Web services and are securely deposited into the consolidated audit service.

Information flow within the VA PIV system is permitted based upon successful matching of identity, access rights validation, and function privilege. An entity must be strongly authenticated to provide assurance of the identity of the operator prior to granting access to a function. An authenticated entity must have approved access rights and the requested function must be appropriate for the role the individual/entity fills to successfully access a requested functionality.

Client services are provided with a session lock and session termination security control that is enforced by the PIV Card. After a specific number of incorrect attempts to access the PIV Card, the device will suspend its operation and require administrative intervention to unlock. This lock mechanism mitigates the risk of a brute-force attack to obtain access to privacy and personal data that is stored on the card. In addition, the PKI services that are integrated with the PIV Card

support session time-out services. These session time-out services must be implemented in the integrated software and application services that use the PKI services (e.g., digital signature and encryption) and are not within the boundary of the PIV system.

The servers that support the IAM components of the VA PIV System are configured to 'lock out" after three minutes of inactivity. These lockouts are enforced by the Windows Operating System. Administrative passwords are required to re-engage the server after it has locked out. Unsuccessful logon attempts are recorded by the operating system and reported to the Audit services of the VA PIV system . After a sufficient number of wrong attempts, the account is locked out and requires a server administrative role to unlock the account. This security control protects against brute-force password guessing and provides protection for the VA PIV System infrastructure instance at the data center.

System Integrity Controls
System Integrity Controls help to ensure that information systems are safe from attacks, intrusions, or unauthorized access attempts from both internal and external sources. This section details the system integrity controls employed on the VA PIV System.

Encryption
The VA PIV System uses a FIPS 140-approved cryptographic module to create encryption keys that support encryption at various levels. Passwords are automatically encrypted when stored. SSH (Secure Shell) encryption keys are used to secure the transfer off data between system components. The SSH keys are created during the time of the production system installation and configuration and are securely stored on each server.

End User/Subscriber encryption key are used to encrypt information and data for users. These encryption key s can be used to secure information in the form of an email, a file, a folder, or grouping of data. These keys are issued to the End User during the registration process. The private decryption key is securely stored on the End Users smart card. The public encryption information is stored in the Shadow Directories to facilitate encrypting communications for other users.

The SSP's CA has a master encryption key that is securely stored on the LUNA CA3 HSM (Hardware Security Module). this key never leaves the HSM device and is used to secure information in the CA internal database. Only the SSP's CA is authorized to encrypt/decrypt database information. The Luna RA is a scalable, high-performance, secure key issuance HSM. It offers FI 140-2 level 2 validation with level 3 validated Random Number Generation (RNG) for secure key generation. The Luna RA fully supports the following hashing algorithms: SHA-1, MD-2, and MD-5. Once a card's issuance sequence is complete, the Lana RA destroys the card 's private key that is stored on the HSM. This enhances the audit ability of the certificate issuance process.

Intrusion Detection and Prevention
A number of elements included in the Va PIV System design will be provided by the Falling Waters and Hines data centers. These elements include: firewalls, network-based IDS (Intrusion Detection System), hot-based IDS, and an IDS Management Console. Each of these components enhances the intrusion prevention levels of the entire system.

Firewall and firewall-based tolls can be configured to detect, block, and notify administrators the intrusion attempts. The firewall units have the ability to detect a number of different attacks, including Denial of Service (DOS) and malformed packet attacks.

IDS Network Sensors are placed in IDS private Network. These units protect against malicious network attack that pass through firewall controls by analyzing various network protocols.

The IDS product will be placed on all servers to provide real-time intrusion protection and detection. These host-based IDS system will analyzed events, host logs, and inbound and outbound traffic to prevent malicious network attacks.

Virus Protection
Virus detection software is part of the base-build for all VA PIV System components. Resident virus scanning is performed on all VA PIV System workstations and servers. Specific details on maintaining the virus signature files will be included in the Operations and Maintenance Plan/Manual. All local drives and file extensions will be scanned on a weekly basis. In addition, all inbound files will be scanned as they are moved to the specific component.
All media to be installed on the VA PIV System must be scanned for known viruses prior to installing such media on the system.

In the event that a virus is detected, the virus protection engine will attempt to clean the virus. A message will be sent to an administrator and a log entry noting the virus detection and subsequent actions. In the event that the engine fails to clean the virus, it will best placed into a designated quarantine area on the server and will be available for further investigation. The specific details concerning the handling of such an alert will be detailed in the Operations and Maintenance Plan/ Manual.

Prevention of Denial of Service Attacks
The security architecture of the VA PIV System significantly reduces the effectiveness of a denial of service attack through

the use of load balancers, Shadow Directories, firewalls, and a Disaster Recovery site located at the Hines Data Center.

The VA PIV System's firewall supports DOS countermeasures. The Firewall Security Appliance scans for more than 55 different attack " signatures" and includes a number of intrusion-prevention features such as Flood guard, DNSGuard, FragGuard, and IPVerify. These tools allow the firewall to look for attacks, block them, and provide real-time notification to administrators. In addition, the VA Enterprise IDS solution will be configured by the data centers to trigger an alert for suspicious activity that matches criteria defined by the VA.

System Banner Messages
Windows 2000 supports configurable access banners (BANNERS_EX). The VA PIV System is configured with the VA standard logon banner. Users are not able to proceed with a session until the access banner is acknowledged by clicking the "OK" button on the screen.

Operating System Security
Windows 2000 provides a security domain for its own protection and provides process isolation. The security domains consist of the following: hardware; kernel-mode software; trusted user mode process; and user-mode administrative tools process. The system hardware is managed by the kernel-mode software and is not modifiable by unauthorized subjects. The kernel-mode software is protected from modification by hardware execution state and memory protection. The hardware provides a software interrupt instruction that causes a state change from user mode to kernel mode. The kernel mode software is responsible for processing all interrupts and determines whether a valid kernel mode call is being made.

Windows 2000 supports the isolation of the Security Support Structure by maintaining a separate security domain for its own execution. The Security domain protects the Security Support Structure from interference and tampering by unauthorized subjects (FPT_SEP.1.1). The Operating System also enforce separation between the security domains of subjects in the system (FPT_SEP.1.2).

Host-based IDs will be configured to recognize normal activity and will alarm for suspicious events outside the parameters of normal activity.

Technical Access Control
Both the Windows 2000 Sever Operating System and Entrust Authority have been tested and certified as enforcing Discretionary Access Control (DAC). The VA PIV System support the following:

. FDP_ACC.1
. FDP_ACF.1.1
. FDP_ACF. 1.2
. FDP_ACF. 1.3
. FDP_ ACF. 1.4

The VA PIV System identifies specific trusted roles the necessary access to accomplished assigned roles. Technical access controls are provided by the OS Windows 2000. Windows 2000 access control controls access to system resources through local system accounts. Specific user rights are controlled throughout New Technology File System (NTFS).

Strong authentication is supported through the use of certificates and the Windows 2000 Operating System security function FIA SOS .1.1 which requires the probability of a random attempt succeeding to be less than one in 250, 000,000,000, 000.

Password Management
Password Management Windows 2000 supports configuration of password policies by an authorized administrator to meet or exceed the VA r requirements. Window 2000 will manage the system passwords for the systems that do not support smart card authentication, SSP's CA, Enterprise Directory and CMS. The systems will strictly use Window 2000 passwords that will be independent of the smart card authentication process. This means the PKI credentials are not being used to logon to the local system or to the network. Users logon to the local system or to the network using their normal Windows 2000 password. The Group Policy for each server has been configured to enforce the VA Password Policy and Password Lifetime.

For the system that do support smart card authentication, the Administrators will create an initial Windows 2000 system account password fo the purpose of enrolling each administrator into each server to which they require access. At the time the user is issued a smart card, he or she will be asked to create a PIN to secure the contents on the smart card. When this Administrator initially; authenticates to each server that requires a smart card, the Administrator will first authenticate to his or her smart card credentials. The user will then be prompted to enter in his or her Windows 2000 system account name and password for the purpose of matching up his or her smart card credentials with the proper system account. From this point forward, the Administrator will not be required to prorvide the Window 2000 system password. The Administrator will only be required to provide the PIN that is used to secure the smart card credentials.

Connections to Non-department Entities

There are no connections outside VA security boundaries for the VA PIV System. Firewalls are employed to segregate the VA PIV System from the rest of the internal VA network. No modems are installed. The VA PIV System enforces group memberships and privileges using the security support structure of the Windows 2000 Operating System.

Operating System Security Auditing
Windows 2000 security audit capability exceeds the level of audit detail specified by the VA requirements. The Operating System also supports Protected Audit Trail Storage (FAU-STG.1) and restricts any modification of the audit log to the role of authorized administrators (FMT_MOF.1(a), FMT_MTD.1(a) and FMT_MTD.1(b). These security requirements are referenced in the "Windows 2000 Security Target: ST Version 2.0;" 18 October 2002 from Microsoft. The Security Audit Logs are routinely backed up and stored off-site for 5 years.

8.2.b) Explain how the project meets IT security requirements and procedures required by federal law.

The VA PIV Project is a Departmental initiative intended to provide compliance with HSPD-12, FIPS 201-1, the Federal Common Policy, and related standards which address the Federal Government need for a standardized identity (PIV) credential to be issued all Federal employees and contractors. Pertinent legislation and guidance driving PIV include, but are not limited to the HSPD 12, FIPS 201-1, OMB M-05-24, E-Government Act of 2002, FISMA/GISRA legislation, the Government Paperwork Elimination Act (GPEA), HIPAA, OMB and National Institute of Standards and Technology (NIST) guidance, and Government Accounting Office (GAO) reports on VA security. Further, PIV program management will work with the PKI Shared Service Provider. The Federal Identity Credentialing Committee has mandated the use of a PKI Shared Service Provider and conformance to the Federal Common Policy. The PIV System is using an approved Shared Service Provider and is in compliance with the Federal Common Policy.
FIPS-201 defines the requirements for the PIV credential enrollment and issuance processes necessary to provide a common assurance level under which all PIV credential are issued.

The VA PIV System will implement PIV Card, PKI and Identity and Access Management services to meet ther requirements of FIPS 201-1. The VA PIV System automates the enrollment and issuance process for the PIV credential, manages the identities of PIV cardholders, manages the lifecycle of the PIV credential, provides data management and provisioning services for interfacing systems, and provides audit and reporting data on PIV System transactions and events.

System Integrity Controls help to ensure that information systems are safe from attacks intrusions, or unauthorized access attempts from both internal and external sources. Here are some examples that identifies how the project meet IT Security Requirements required by federal law:

Encryption
The VA PIV System uses a FIPS 140 approved cryptographic module to create encryption keys that support encryption at various levels. Passwords are automatically encrypted when stored. SSH (Secure Shell) encryption keys are used to secure the transfer of data between system components. The SSH keys are created during the time of the production system installation and configuration and are securely stored on each server.

The federally approved SSP's CA has a master encryption key that is securely stored on the LUNA CA3 HSM (Hardware Security Module). Only the SSP's CA is authorized to encrypt/decrypt database information. The Lunar RA is a scalable, high performance, secure key issuance HSM which offers FIPS 140-2 level 2 validation with level 3 validated Random Number Generation (RNG) for secure key generation, supporting the following NIST approved hashing algorithms: SHA-1, MD-2, and MD-5.

Security Subsystem
The Security Sub-system of the VA PIV System is a critical component that protects sensitive, privacy, and agency restricted data. This sub-system provides the compliance mechanism for the Federal Information Security Management Act of 2002. (FISMA) and provides the assurance that the data collected and used and stored by the system is protected at an appropriate level to restrict unauthorized access to sensitive information.

9. CHANGE RECORD

OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, mandates that PIAs address any project/ system changes that potentially create new privacy risks. By completing this section, you provide documented assurance that significant project/ system modifications have been appropriately evaluated for privacy-related impacts.

9.a Since the last PIA submitted, have any significant changes been made to the system that might impact the privacy of people whose information is retained on project systems? (Yes, No, n/a: first PIA)

No

If no, then proceed to Section 10, "Children's Online Privacy Protection Act."

If yes, then please complete the information in the table below. List each significant change on a separate row. 'Significant changes' may include:

Conversions - when converting paper-based records to electronic systems;

Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;

Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:

• For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist.

Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated:

• For example, when databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns not previously at issue.

New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;

Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);

New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;

Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:

• For example, agencies that participate in E-Gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or E-Gov requirements. In most cases the focus will be on integration of common processes and supporting data. Any business change that results in substantial new requirements for information in identifiable form could warrant examination of privacy issues.

Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information);

List All Major Project / System Modification(s)	State Justification for Modification(s)	*Concisely describe:	Modification Approver	Date

**• The effect of the modification on the privacy of collected personal information*

**• How any adverse effects on the privacy of collected information were mitigated.*

10. CHILDREN'S ONLINE PRIVACY PROTECTION ACT

10.a) Will information be collected through the Internet from children under age 13?

No

If "No" then SKIP to Section 11, "PIA Considerations".

10.b) How will parental or guardian approval be obtained.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

11. PIA CONSIDERATIONS

11) Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA. Examples of choices made include reconsideration of: collection source, collection methods, controls to mitigate misuse of information, provision of consent and privacy notice, and security controls.

This is the second PIA performed on the PIV system. Future consideration's to subsequent PIV system design or operations will be made with full consideration of IA impact.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

12. PUBLIC AVAILABILITY

The Electronic Government Act of 2002 requires that VA make this PIA available to the public. This section is intended to provide documented assurance that the PIA is reviewed for any potentially sensitive information that should be removed from the version of the PIA that is made available to the public.

The following guidance is excerpted from M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," Section II.C.3, "Review and Publication": iii. Agencies must ensure that the PIA document and, if prepared, summary, are made publicly available (consistent with executive branch policy on the release of information about systems for which funding is proposed).

1. Agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment9. Such information shall be protected and handled consistent with the Freedom of Information Act (FOIA).

2. Agencies should not include information in identifiable form in their privacy impact assessments, as there is no need for the PIA to include such information. Thus, agencies may not seek to avoid making the PIA publicly available on these grounds.

12.a) Does this PIA contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?

No

12.b) If yes, specify:

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

13. ACCEPTANCE OF RESPONSIBILITY AND ACKNOWLEDGEMENT OF ACCOUNTABILITY:

13.1) I have carefully reviewed the responses to each of the questions in this PIA. I am responsible for funding and procuring, developing, and integrating privacy and security controls into the project. I understand that integrating privacy and security considerations into the project may affect the development time and cost of this project and must be planned for accordingly. I will ensure that VA privacy and information security policies, guidelines, and procedures are followed in the development, integration, and, if applicable, the operation and maintenance of this application.

Yes

13.2) Project Manager/Owner Name and Date (mm/dd/yyyy)

Brian Epley 08/22/2007

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)