

Privacy Impact Assessment - 2009 (Form) / Document and Correspondence Management System (DCMS)-2009 (Item)

Part I. Project Identification and Determination of PIA Requirement

1. PROJECT IDENTIFICATION:

1.1) Project Basic Information:

1.1.a) Project or Application Name:

Document and Correspondence Management System (DCMS)-2009

1.1.b) OMB Unique Project Identifier:

029-00-03-00-01-1016-00

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.

The Document and Correspondence Management System (DCMS) project is proposed to replace the Electronic Document Management System (EDMS), VA's current system, with updated technology. DCMS, a web-based, scalable COTS solution, will enhance the essential functionality to manage executive level correspondence and controlled documents, by providing effective search and management reporting capabilities, e-mail notification capabilities, & access/security restrictions for a variety of sensitive actions and documents.

There is a performance gap with regard to a reliable & flexible Agency correspondence system. This function is essential to the Office of the Secretary, VA White House Liaison, and VA Office of Congressional and Legislative Affairs. DCMS will reduce and eventually eliminate this gap by providing essential functionality to manage executive level correspondence through tracking accountability, workflow distribution flexibility, form letters, electronic signature capabilities, & controlled documents & assignments, meeting the business need of VA's executives.

Web-based facilitated correspondence supports PMA & E-Gov initiatives. DCMS supports strategic Objective E-3. Specifically, DCMS will enable VA to: better manage informed, timely, accurate, & consistent correspondence responses to veterans, their families, Congress, and the White House; smooth workflow within CO and between CO and VA field offices; implement a secure structure for correspondence management that allows for storage of data while restricting access; and eliminate need for redundant systems in VA administrations.

DCMS is a veteran-centric approach to meeting VA's correspondence needs and is the foundation of the Secretary's correspondence priorities, for faster responses to Veteran's & families. DCMS meets Objective E-2. This is accomplished by providing automated communication to veterans & their families through faster response to correspondence.

While there is recognition of the priority of OMB money to support DCMS, funding will be supplemented. The system is essential to VA upper level management nationwide, to keep pace & respond to VA correspondence and decisions. Because it is vital in advancing agency communications, moneys will be transferred from the various parts of VA to support DCMS.

In 2005 the Secretary's Office funded up to \$250,000; in 2006, it was funded up to \$1.92M; in 2007, it was funded up to \$2.159M.

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.

The existing EDMS architecture limits the user base to VACO. Users outside of VACO track correspondence in other systems or manually. This has led to redundant and often inconsistent tracking of correspondence and difficulties in ensuring accountability of VA offices and individuals. The lack of direct access by VA field offices prevents effective integration of all business lines and staff offices into a comprehensive correspondence and document workflow to prepare and track executive level and controlled documentation. Other notable issues with the current environment include the lack of essential functionality, including effective search and management reporting capabilities, document versioning, meaningful and correct status tracking, and seamless integration with e-mail capabilities and standard office automation products. The current EDMS also does not provide access restriction that would permit EDMS to be used for a variety of sensitive actions and documents. Finally, the system's outdated technology is highly vulnerable to system failure, is no longer supported by the software vendor, and is difficult to use and maintain, preventing a large number of staff to be integrated into an automated document workflow.

The DCMS presents an opportunity to implement modern document management technology at VA and to solve the following business and technical problems:

- Support of VA's business needs through modern workflow and document handling capabilities that will improve correspondence/document process, reduce turnaround time of reviews and concurrences, and improve overall services to correspondence.
- Direct access to information and data required by all offices and individuals supporting VA Central Office (VACO) executive-level correspondence and document needs.
- Better control, oversight and accountability of all offices and individuals involved in the document and correspondence process
- Improved control over documents and efficient archiving capabilities
- Reduced data redundancy by storing information in one central system
- Current technology to eliminate the vulnerability of technical failure.

The DCMS project seeks to solve current business, technical, and security inadequacies through a web-based, scalable COTS solution that can be easily used by staff and management throughout the VA, regardless of where documents originate or users reside. The project is in the Operations/Maintenance phase. The operational system will be implemented Phase 2 for up to 2,000 users, including VACO and four field offices. VA is contemplating a Phase 3 to implement this highly scalable system further in the field as an enterprise-wide solution for document management.

1.2) Contact Information:

| | |
|--|--|
| 1.2.a) Person completing this document: | Vicki Cordes |
| Title: | Information Technology Specialist |
| Organization: | Office of Information and Technology, Office of Enterprise Development, Resource Management Information Technology (005Q3) |
| Telephone Number: | 202-461-9034 |
| Email Address: | Vicki.Cordes@va.gov |
| 1.2.b) Project Manager: | Vicki Cordes |
| Title: | Information Technology Specialist |
| Organization: | Office of Information and Technology, Office of Enterprise Development, Resource Management Information Technology (005Q3) |
| Telephone Number: | 202-461-9034 |
| Email Address: | Vicki.Cordes@va.gov |
| 1.2.c) Staff Contact Person: | Adam Evans |
| Title: | Information Technology Specialist |
| Organization: | Office of Information and Technology, Office of Enterprise Development, Resource Management Information Technology (005Q3) |
| Telephone Number: | 202-461-9263 |
| Email Address: | Adam.Evans@va.gov |
| | |

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

N/A

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?

Yes

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

No

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.)

N/A

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.

To process replies to correspondence and other inquiries (received via hard copy, e-mail, fax, Internet, telephone, or in person) that originate from Members of Congress; other Federal agencies; state, local and tribal governments; Foreign governments; veterans service organizations; representatives of private or commercial entities; veterans and their beneficiaries; other private citizens; and VA employees.

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

No specific legal authority.

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) Operations/Maintenance

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.

DCMS will be operational for VACO by the end of FY 2008.

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

N/A

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. |
| Yes |
| 4.b.1) For each applicable System of Records, list: |
| (1) The System of Records identifier (number), |
| EDMS 92VA045 |
| (2) The name of the System of Records, and |
| Document and Correspondence Management System (DCMS) |
| (3) Provide the location where the specific applicable System of Records Notice(s) may be accessed (include the URL). |
| www.gpoaccess.gov |
| 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. |
| Electronic Document Management System (EDMS) is the current system being replaced by the Document and Correspondence Management System (DCMS). The System of Records contains individually identifiable data of the public (such as name, address, telephone number, e-mail address, etc.) that were created and used for EDMS and will be migrated to DCMS for its use. |
| 4.b.4) Does the System of Records Notice require modification? |
| If "No" then skip to section 5, 'Data Collection'. |
| No, at this time it does not appear the System of Records Notice requires modification. However, we will perform a review to ensure that a modification is not required. |
| 4.b.5) Describe the required modifications. |
| |
| 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: |
| N/A |
| ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.) |
| N/A |
| PIA SECTION 5 |

| |
|---|
| Project Name |
| Document and Correspondence Management System (DCMS)-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 Information of the veteran or primary personal contact may contain name, address, phone number, and e-mail address. Information is provided by the individual voluntarily and is used to efficiently track and manage timely, accurate, and consistent correspondence responses to veterans, their families, Congress, the White House, citizens, and other Federal agencies. DCMS is used to process replies to correspondence and other inquiries that originate from Members of Congress; other Federal agencies; state, local, and tribal governments; Foreign governments; veterans service organizations; representatives of private or commercial entities; veterans and their beneficiaries; private citizens; and VA employees. DCMS is also used for some categories of correspondence and records internal to VA.

| | |
|-----|---|
| Yes | Other Personal Information of the Veteran or Primary Subject |
|-----|---|

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

Other personal information of the veteran or primary personal contact may contain social security number or date of birth. Information is provided by the individual voluntarily and is used to respond to inquiries and/or requests and to efficiently track and manage timely, accurate, and consistent correspondence responses to veterans, their families, Congress, the White House, citizens, and other Federal agencies.

| | |
|-----|------------------------------|
| Yes | Dependent Information |
|-----|------------------------------|

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

Dependent information may contain name, address, phone number, and e-mail address. Information is provided by the individual voluntarily in order to efficiently respond to his/her request.

| | |
|-----|----------------------------|
| Yes | Service Information |
|-----|----------------------------|

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

Service information may contain years and name of the unit service entity. Information is provided by the individual voluntarily in order to efficiently respond to his/her request.

| | |
|-----|----------------------------|
| Yes | Medical Information |
|-----|----------------------------|

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

Medical information may contain medical reports, prescription information, and psychiatric diagnosis. Information is provided by the individual voluntarily in order to efficiently respond to his/her request.

| | |
|-----|------------------------------------|
| Yes | Criminal Record Information |
|-----|------------------------------------|

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

Personal information may contain police/criminal report. Information is provided by the individual voluntarily in order to efficiently respond to his/her request.

| | |
|-----|-----------------------------|
| Yes | Guardian Information |
|-----|-----------------------------|

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

Guardian information may contain name, address, phone number, and e-mail Address. Information is provided by the individual voluntarily in order to efficiently respond to his/her request.

| | |
|-----|------------------------------|
| Yes | Education Information |
|-----|------------------------------|

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

Education information may contain the individual's highest education level. Information is provided by the individual voluntarily in order to efficiently respond to his/her request.

| | |
|-----|-----------------------------------|
| Yes | Rehabilitation Information |
|-----|-----------------------------------|

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

Rehabilitation information may contain the details of the veteran's rehabilitation history. Information is provided by the individual voluntarily in order to efficiently respond to his/her request.

| | |
|-----|--|
| 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.

Other personal information may indirectly contain the individual's gender, race, financial status, marital status, employment status, or political affiliation. Information is provided by the individual voluntarily in order to efficiently respond to his/her request.

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

N/A

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.

Yes

Veteran Source

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

Veterans writing to the VA voluntarily provide their contact information (address, phone number, and/or e-mail address) to receive an expedient response to their correspondence request. Correspondence may contain other personal information as described in Section 5.1.

Yes

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.

Members of the public writing to the VA voluntarily provide their contact information (address, phone number, and/or e-mail address) to receive an expedient response to their correspondence request. Correspondence may contain other personal information as described in Section 5.1.

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.

No

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.

| | |
|----|-------------------------------|
| 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.

| | |
|----|------------------------|
| No | 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.

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

N/A

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.

| | | |
|----|-------------------|--|
| No | 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.")

| | | |
|--|--|--|
| | | |
|--|--|--|

| | | |
|-----|---------------------|--|
| 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.

No form is used to collect information. Information is recorded from letters or memoranda collected by the Department.

| | | |
|----|----------------------------------|--|
| No | Electronic File Transfer: | Information stored on one computer/system (not entered via a Web Form) and 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.)

| | | |
|----|----------------------------------|--|
| No | 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.

| | | |
|-----|---------------------------|---|
| Yes | Telephone Contact: | Information is collected via telephone. |
|-----|---------------------------|---|

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

Should additional information be necessary for the VA to provide an adequate and appropriate response to the correspondent, the VA program office may make contact via phone to obtain the necessary information from the correspondent. Information obtained via telephone is then entered into DCMS.

| | | |
|----|---------------------------------|--|
| No | Other Collection Method: | Information is collected through a method other than 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.

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

N/A

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?

Yes

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

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

Voluntary

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?

The individuals are voluntarily providing the VA personal contact information in order to receive a response to their correspondence.

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.)

| | |
|----|--|
| No | Not applicable |
| | Privacy notice is provided on each page of the application. |
| | A link to the VA Website Privacy Policy is provided. |
| | Proximity and Timing: the notice is provided at the time and point of data collection. |
| | Purpose: notice describes the principal purpose(s) for which the information will be used. |
| | Authority: notice specifies the legal authority that allows the information to be collected. |
| | Conditions: notice specifies if providing information is voluntary, and effects, if any, of not providing it. |
| | 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:

N/A

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.

| | |
|----|-------------------|
| No | 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.

| | |
|-----|---------------------|
| 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.

Individuals voluntarily provide information in paper forms (i.e., letters) to the VA, in pursuit of getting their needs/requests addressed. Privacy notice is provided via the Internet site (<http://www.va.gov/privacy/>) and published in the Federal Register.

| | |
|----|----------------------------------|
| 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?

| | |
|----|----------------------------------|
| No | 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?

| | |
|-----|-------------------|
| Yes | 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.

Individuals voluntarily provide information via telephone calls to the VA, in pursuit of getting their needs/requests addressed. Privacy notice is provided via the Internet site (<http://www.va.gov/privacy/>) and published in the Federal Register.

| | |
|----|----------------------|
| No | 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.)

N/A

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:

Only the personal information directly provided by the correspondent can be entered into the system. The system requires the user to perform an initial search to determine if the correspondent already exists in the database before entering data into the system.

5.6.b) How is data checked for completeness?

After entry, the record is checked against a third party address verification system/software.

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

If the correspondent writes again, the information is verified against the existing record and updated as necessary.

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

Same as above

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

N/A

PIA SECTIONS 6 - 13

Project Name

Document and Correspondence Management System (DCMS)-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.

Lockheed Martin Information Technology (LMIT) is the vendor that entered into a contractual agreement with the VA to provide the VA a Document and Correspondence Management System (DCMS). LMIT will support the VA with maintenance of the system for 1 year after the Phase 3 implementation, during which time they will have access to all data in the database to operate the DCMS. LMIT staff with access are required to complete the mandatory VA security awareness training and undergo background check. Contract #: GS-35F-0636K

| | |
|-----|---|
| Yes | 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.

VACO, VHA, VBA, NCA, and field offices (regional offices, VHA Medical Centers, VA outpatient clinics, Veterans Integrated Service Network (VISN) offices, and NCA Memorial Service Network (MSN) offices. The expansion of DCMS to VA field offices reduces the need for redundant systems, and allows for more consistent and accurate method of collaborating on responses to correspondence.

| | |
|-----|-----------------------------------|
| Yes | 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.

We are sharing information in response to the Veterans organizations' written request in accordance with the routine uses in the published System of Records Notice. Information may be provided to a third party acting on an individual's behalf, such as agencies of Federal, state, local and tribal governments, Foreign governments; veterans service organizations; representatives of private or commercial entities in response to a request made by the individual to the third party and concerning that individual's VA records. Such information will be provided as authorized by law.

| | |
|-----|--|
| 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.

The White House, Members of Congress, and other Federal agencies may refer correspondence to the VA that falls within the VA jurisdiction. VA would provide the referring agency office with notice or copy to indicate that the response was provided to their constituent.

VA may disclose the records in this system that it determines are relevant to a suspected violation or reasonably imminent violation of law, whether civil, criminal or regulatory in nature, and whether arising by general or program statute or by regulation, rule or order issued pursuant thereto, to a Federal, state, local, tribal or foreign agency charged with the responsibility of investigating or prosecuting such violation, or charged with enforcing or implementing the statute, regulation or order issued pursuant thereto.

VA may disclose the records in proceedings before a court or adjudicative body before which VA is authorized to appear when VA, a VA official or employee, the United States, or an individual or entity for whom the United States is providing representation is a party to litigation or has an interest in such litigation, and VA determines that the use of such records is relevant and necessary to the litigation, provided, however, that in each case, the agency determines that disclosure of the records is a use of the information contained in the records that is compatible with the purpose for which the records were collected.

Information may be provided to Members of Congress or staff persons in response to an inquiry from an individual to Members of Congress, made at the request of the individual and concerning that individual's VA records. Such information will be provided as authorized by law.

Information may be provided to a third party acting on an individual's behalf, such as agencies of Federal, state, local and tribal governments, Foreign governments; veterans service organizations; representatives of private or commercial entities in response to a request made by the individual to the third party and concerning that individual's VA records. Such information will be provided as authorized by law.

VA may compile statistical information using records contained in DCMS, except for identification information of a veteran such as name, address or social security number. This information may be disclosed to other VA facilities, Members of Congress; other Federal agencies; state, local and tribal governments. VA will determine that the use of such statistical information is relevant and necessary, and that disclosure of the information contained in the records is compatible with the purpose for which the records were collected.

Disclosure may be made during reviews by the National Archives and Records Administration in records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

VA may disclose relevant information to the Department of Justice and United States Attorneys in defense or prosecution of litigation involving the United States.

| | |
|-----|--------------------------------|
| Yes | 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.

Same as above

| | |
|-----|--------------------------------|
| Yes | 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.

Same as above

| | |
|----|------------------------------|
| 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:

System users, system administrators, LMIT contractors

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

The access to the data will be authenticated by the user ID and the user group the user belongs to, as defined in the user profile table.

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

Documentation prepared in Phase I of the project included a Project Charter and System Security Plan that identified roles, responsibilities, procedures, and security and access controls. DCMS implementation at VACO will now occur in Phase 2. Documentation from Phase 1 will be reviewed and finalized in Phase 2.

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

Level of access to the system data will be determined/restricted based on the user ID and the user group. Access to the record is provided on a "need to know" basis.

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)

Users must sign the Rules of Behavior prior to receiving access to data in the system. In addition, users must complete mandatory security and privacy awareness training.

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)

Yes

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.

Release of personally identifiable information will only be made in accordance with the provisions of the Privacy Act of 1974, for investigatory, judicial and administrative uses. This includes disclosure to third parties acting on a claimant's behalf; to law enforcement agencies when records in the system pertain to a violation or possible violation of law; to answer congressional inquiries initiated by individuals; to the National Archives and Records Administration during records management inspections; to requests for statistical data to be disclosed to other VA facilities; Members of Congress; other Federal agencies; state, local and tribal governments for statistical analyses. VA has determined that release of information for these purposes is a necessary and proper use of information in this system of records and that specific routine uses for transfer of this information are appropriate. Information is only shared in an effort to respond to an individual's request or when meeting a routine use of the System of Records Notice. Additionally, VA has a number of policies in place for protecting personally identifiable information (PII) and DCMS adheres to these policies in an effort to protect this information from unauthorized access and use.

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

VA Privacy Officers are responsible for monitoring their facility's compliance with privacy requirements, as well as receiving and processing complaints from Veterans and other individuals regarding privacy violations. Additional duties

vary by facility and Administration, but could include:

- Accounting of Disclosures
- Privacy Training
- Amendment of Records
- Privacy Expertise
- FOIA
- Privacy Marketing
- Information Disposition
- Release of Information
- Information Life Cycle
- Requests for Access to Information
- System of Records
- Working with the Information Security Officer

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

For the Phase 2 VACO implementation of DCMS, only persons holding VA internally issued licenses will have access to the DCMS system and data. Because DCMS will be a closed system in the Phase 2 VACO implementation, no personal information will be transmitted via e-mail. Correspondence outside of VACO and with outside entities such as Congress or other Federal agencies are handled by local office correspondence policies and procedures.

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.

It is covered by routine use in the System of Records Notice.

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

By applying the record security controls with the document and correspondence management system.

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

N/A

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

N/A

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.)

| | |
|-------------------------------------|--|
| <input type="checkbox"/> | The application will provide a link that leads to their information. |
| <input type="checkbox"/> | The application will provide, via link or where data is collected, written instructions on how to access/amend their information. |
| <input checked="" type="checkbox"/> | The application will provide a phone number of a VA representative who will provide instructions. |
| <input type="checkbox"/> | The application will use other method (explain below). |
| <input type="checkbox"/> | 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?

Submit a FOIA request or write comments, suggestions, or objections to the Associate Deputy Assistant Secretary for Privacy and Records Management (005R1), Department of Veterans Affairs, 810 Vermont Ave., NW, Washington, DC 20420--(202) 461-7453.

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

Write to the contact the Associate Deputy Assistant Secretary for Privacy and Records Management (005R1), Department of Veterans Affairs, 810 Vermont Ave., NW, Washington, DC 20420--(202) 461-7453.

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.*

N/A

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

N/A

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.*

As part of DCMS Phase 2, records retention will be addressed in accordance with the applicable Records Control Schedule. All documents pertaining to data retention procedures will be developed.

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

As part of DCMS Phase 2, records retention will be addressed in accordance with the applicable Records Control Schedule. All documents pertaining to data retention procedures will be developed.

7.c) *Where are procedures documented?*

N/A

7.d) *How are data retention procedures enforced?*

N/A

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

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

N/A

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:

System administrators periodically monitor and test security applied within the application.

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? If so, describe these controls.

The access to the information in DCMS will be authenticated by the user ID and password of the user as defined in the DCMS user profiles. After the user authentication succeeds and the user enters the system, the group(s) user belongs to and the user's established access level (read only, edit, full) for record security will determine if the user will be able to read, modify or create records. In DCMS, any action taken by a system user is logged in an audit trail for accountability.

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

Prior to production, a Certification and Accreditation with the Authority to Operate will be complete.

Prior to receiving access, the user must complete and sign User Access Request Form. The user acknowledges and signs he/she will abide by the Rules of Behavior. The user also must complete mandatory security and privacy awareness training. Separate Rules of Behavior will be established for the application/system administrators with privileged accounts, including application, database, and alternate system administrators.

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)

Yes

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 |
|---|---|--|------------------------|--------|
| DCMS Phase 2 | DCMS replaces VA's current Electronic Document Management System (EDMS) with updated technology. DCMS is a web-based, scalable COTS solution, which will enhance the essential functionality to manage executive level correspondence and controlled documents by providing effective search and management reporting capabilities, e-mail notification capabilities, and access/security restrictions for a variety of sensitive actions and documents. DCMS Phase 2 VACO implementation will be a closed system. Only VA licensed users will have access to the DCMS system and data. | With the closed system to be implemented in DCMS Phase 2 VACO, personally identifiable information (PII) will be contained within the application and accessed only by licensed DCMS application users. Correspondence with the field and outside entities will continue to be handled by the local office correspondence policies and procedures. | Executive Secretariate | FY '08 |
| | | | | |
| | | | | |

| | | | | |
|--|--|--|--|--|
| | | | | |
| | | | | |

* 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.

N/A

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

N/A

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.

As a result of performing the PIA, the project team became more aware of the importance of the provision of consent and privacy notice, and will enforce the completion of the privacy notice by the system users when the system is implemented.

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

The access controls will be documented in Phase 2. The Records Control Schedule and Procedures will be identified in Phase 2.

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)

IT Project Manager: Vicki Cordes, OI&T, Office of Enterprise Development (OED), Resource Management IT (005Q3), 9/21/2007

Owner: Joseph Bond, OI&T, Office of Enterprise Development (OED), Resource Management IT (005Q3), 9/21/2007

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

| |
|--|
| |
|--|