Privacy Impact Assessment for the VA IT System called:

Environmental Agents Service Registries (EAS)

28 April 2015

VA System Contacts:

	Name	E-mail	Phone Number
Privacy Officer	Mark Littlefield Artur Tocilla	mark.littlefield@va.gov artur.tocilla@va.gov	708-681-6773 215-842-2000 x4724
Information Security Officer	Stephan Chan	stephan.chan@va.gov	(202) 632-7393
System Owner	Tammy Watson	tammy.watson@va.gov	(202) 461-6126
Person Completing the Document	Martha Clark	martha.clark4@va.gov	(512) 326-6031

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system.
- A general description of the information in the IT system.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- A citation of the legal authority to operate the IT system.

Environmental Agents Service Registries (EAS) is a web-based standardized methodology for processing and storing specific medical and demographic data related to the examination of veterans and veterans' dependents. It is a combination of application inputs for Agent Orange, Persian Gulf War, Depleted Uranium, and Ionizing Radiation registries. Eligibility status is dictated under Title 38 United States Code. In addition, certain VHA directives establish the programs and protocols for operation. This includes, but is not limited to: VHA1301 (IRD), Public Laws 102-585 and 100-687 (Agent Orange), Public Law 102-190 (Gulf War), Public Law 103-445 and VHA Directive 99-019 (Gulf War Dependents), and VHA Directive 98-032 (Depleted Uranium).

EAS data is collected in a structured approach for staff to gather information on a patient's history and complaints followed by clinician examination and diagnosis. The purpose of EAS is to collect and store the information so that it may be used for studies of patterns of war-related diseases and in some cases, determination of benefits eligibility. EAS then populates demographic and health information from National Medical Information Systems (NMIS) database, National Patient Care (NPC), in a one-way (read only) connection. In addition, new patients are added to the newsletter mailing list based on the agent they are being seen for. The mailing list is provided to the Veterans Affairs (VA) Central Office where the newsletters originate.

EAS users log on using the Customer User Provisioning System (CUPS) assigned user-id and EAS website password. CUPS is used for requesting and monitoring user access to AITC computer resources. Once logged on, the user can access existing EAS registries and add new ones. The demographic service and health data is captured from NPC when the user adds a veteran to the database. A validation process is performed on the Web server when the user saves any changes to a new or existing exam. If the information is found to be valid, the EAS database is updated with the new data. Otherwise, the user is prompted to make corrections before data can be saved. Approximately 191 VHA facilities, mainly consisting of Veterans Health Administration (VHA) outpatient clinics, collect EAS data via the EAS website.

Veterans use the www.EasMailCall.aac.va.gov and provide an email address and select from 1 to 4 newsletters which are collected in a file on the EAS web server. These entries are then stored in the EAS Newsletter database. The EAS Newsletter database provides a list of email addresses and the listed Veterans are sent a link to an online version of the Newsletter(s) selected.

Section 1: Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see the VA Handbook 6500 (http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=638&FType=2), published Sept. 2012, Appendix A.)

If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Mailing Address
- ☒ Zip Code
- ☒ Phone Number(s)
- ☐ Fax Number
- ☒ Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc of a different individual)
- ☒ Financial Account Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Current Medications
- ☐ Previous Medical Records
- ☐ Race/Ethnicity

Other information maintained in the system: Agent Orange registry, Gulf War and Gulf War Dependents registries, Depleted Uranium registry, Ionizing Radiation registry, medical history and condition, symptoms and diagnosis.

1.2 What are the sources of the information in the system?

List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

VA Health Clinic clinicians gather patient history and complaint information and store it in EAS so that it may be used for studies of patterns of war-related diseases and in some cases, determination of benefits eligibility. EAS also pulls demographic and health history from the NPC database using a one-way connection.

Demographic (name, address, spouse, children, parents, grandparents, etc.) information is collected from NPC/the patient and retained in the EAS database table: Patient.

Service Information is collected from NPC and retained in the EAS database table: Period of Service.

Health Information is collected from NPC/the patient/VA Health Clinic and retained in the EAS database tables: AO Exam, GW Exam, GWII Exam, DU Exam, IR Exam, Diagnosis, and Symptom.

1.3 How is the information collected?

This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.

No form is used; it is collected in the EAS application itself from the patient by the clinician and from the NPC one-way connection for demographic and health information and retained in the appropriate database tables.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publically available or commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose.

The information collected is entered into specific fields of the EAS database in support of studies of patterns of war-related diseases and in some cases, determination of benefits eligibility. The veteran information is to determine eligibility and entitlement for VA compensation and pension benefits and the veteran's family relation or guardian (spouse, children, parents, grandparents, etc.) information is to designate a VA guardian to manage the VA compensation and pension benefits of those individuals who are not competent to manage their own funds for VA entitlement purposes.

1.5 How will the information be checked for accuracy?

Discuss whether and how information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency?

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

Veteran data is checked for completeness by manual verifications, and mailed registration forms through automated veteran newsletters. These forms ask for specific information for verification. The correspondence from each veteran is then used to update the data in the newsletter database.

1.6 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.

The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38 United States Code, VHA directive 1301 (Ionizing Radiation Registry), Public Laws 102-585 (Veterans Health Care Act of 1992) and 100-687 (Agent Orange Act of 1991), Public Law 102-190 (Gulf War), Public Law 103-445 and VHA Directive 99-019 (Gulf War Dependents), and VHA Directive 98-032 (Depleted Uranium).

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for DHS to ensure that personally identifiable information is accurate, complete, and current?

Follow the format below when entering your risk assessment:

Privacy Risk: The EAS application collects Personally Identifiable Information (PII) and other highly delicate Sensitive Personal Information (SPI). If this information were to be breached or accidentally released inappropriately, it could result in the financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: The VA is careful to only collect the information necessary to identify the veteran, identify the potential issues and concerns, and offer assistance to the Veteran so that they may find the help needed. By only collecting the minimum necessary information, the VA is able to better protect the Veterans' information.

Section 2: Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained.

Name: Used to identify Veteran.

Social Security Number: Used to verify identity of Veteran.

Date of Birth: Used to verify identify of Veteran.

Mailing Address: Used to verify identity of Veteran.

Zip Code: Used to verify identify of Veteran

Spouse: Used to identify dependent or possible Veteran guardian.

Children: Used to identify dependent or possible Veteran guardian.

Parents: Used to identify possible Veteran guardian.

Grandparents: Used to identify possible Veteran guardian.

Service Information: Used to verify eligibility of Veteran and identified dependents.

Health Information: Used to record health history/medical conditions and symptoms of the Veteran.

Financial information: Used in the event eligibility is verified for VA benefits.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

EAS does not analyze patient data. It does collect and store it for use in war-related diseases pattern analysis studies. A goal for EAS is to provide a structured approach for gathering information on a patient's history, symptoms, and complaints for: Agent Orange registry, Gulf War and Gulf War Dependents registries, Depleted Uranium registry, and Ionizing Radiation registry.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. *Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.*

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?

The official System of Records Notices (SORNs) for EAS are:

"National Patient Databases-VA" (121VA19) at http://www.gpo.gov/fdsys/pkg/FR-2010-11-26/pdf/2010-29695.pdf

"Agent Orange Registry" (105VA131) at http://www.gpo.gov/fdsys/pkg/FR-2009-03-16/pdf/E9-5598.pdf

"Gulf War Registry" (93VA131) at http://www.gpo.gov/fdsys/pkg/FR-2015-03-03/pdf/2015-04313.pdf

"Ionizing Radiation Registry" 69VA131 at http://www.gpo.gov/fdsys/pkg/FR-2008-12-08/pdf/E8-29016.pdf

Section 3: Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is retained by the system.

EAS retains Demographic (name, address, spouse, children, parents, grandparents, etc.), Service Information, Health Information and Financial Information.

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods.

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.

Electronic Data remains in the database permanently. There is no paper record as all interview information is entered electronically.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.

The data retention schedule is detailed in the VA Record Control Schedule 10-1, dated March 1, 2011.

http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.

There is no elimination of SPI; all information is permanent.

3.5 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

Follow the format below:

Privacy Risk: All information is kept permanently.

Mitigation: In order to operate, EAS must meet all security requirements outlined in the Authority to Operation accreditation process. This included continuous monitoring as part of the Continuous Readiness in Information Security Program (CRISP). This includes regular scans and remediation tracking.

Section 4: Internal Sharing and Disclosure

The following questions are intended to define the scope of information sharing within VA.

4.1 With which internal organizations is information shared? What information is shared, and for what purpose? How is the information transmitted or disclosed?

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific information is shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

Program Office or IT System information is shared with	Reason why information is shared with the specified program or IT system	List the specific information types that are shared with the Program or IT system	Method of transmittal
National Patient Care (NPC) Database	Shared information is used for pattern analysis, eligibility, and entitlement.	Demographic, Service and Health information	EAS captures NPC information electronically as a new entry is made for a veteran. The PII information is validated and cannot be saved unless EAS has the correct information.
Veterans Affairs Central Office (VACO)	Information is used to mail newsletter(s) to Veteran	Name and Address	Electronic mailing list containing Veteran name, address and newsletter(s) selected is provided to VACO to mail newsletters.
Customer User Provisioning System (CUPS)	Information is used to provide User access to EAS	Name to get user ID and EAS password	Information is transmitted via email but process is outside the EAS accreditation boundary.
Environmental Agent: Agent Orange	Newsletter that can be provided to the Veteran	Name, address or email address	Provided electronically in a mailing list to VACO or by Veteran to receive link to online newsletter
Environmental Agent: Persian Gulf War	Newsletter that can be provided to the Veteran	Name, address or email address	Provided electronically in a mailing list to VACO or by Veteran to receive link to online newsletter
Environmental Agent: Depleted Uranium	Newsletter that can be provided to the Veteran	Name, address or email address	Provided electronically in a mailing list to VACO or by Veteran to receive link to online newsletter
Environmental Agent: Ionizing Radiation	Newsletter that can be provided to the Veteran	Name, address or email address	Provided electronically in a mailing list to VACO or by Veteran to receive link to online newsletter

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Follow the format below:

Privacy Risk: There is a risk that data contained in EAS may be shared with unauthorized individuals or that those individuals, even with permission to access the data, may share it with other individuals.

Mitigation: All users of the system are VA users. All VA users are trained and acknowledge usage requirements in the appropriate Rules of Behavior (RoB) documentation. Access to veteran data for use is under Title 38 U.S.C. Section 5106.

Section 5: External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations is information shared? What information is shared, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific information is shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

Program Office or IT System information is shared with	Reason why information is shared with the specified program or IT system	List the specific information types that are shared with the Program or IT system	Legal authority, binding agreement, SORN routine use, etc that permit external sharing (can be more than one)	Method of transmission and measures in place to secure data

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

Follow the format below:

Privacy Risk: There are no external connections to EAS. All connections are VA internal.

Mitigation: There are no external connections to EAS. All connections are VA internal.

Section 6: Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information?

This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register. If notice was provided in the Federal Register, provide the citation.

If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

The notice is provided to the veteran verbally. The official SORNs for EAS are:

"National Patient Databases-VA" (121VA19) at http://www.gpo.gov/fdsys/pkg/FR-2010-11-26/pdf/2010-29695.pdf

"Agent Orange Registry" (105VA131) at http://www.gpo.gov/fdsys/pkg/FR-2009-03-16/pdf/E9-5598.pdf

"Gulf War Registry" (93VA131) at http://www.gpo.gov/fdsys/pkg/FR-2015-03-03/pdf/2015-04313.pdf

"Ionizing Radiation Registry" 69VA131 at http://www.gpo.gov/fdsys/pkg/FR-2008-12-08/pdf/E8-29016.pdf

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached.

Veterans have the right to decline to provide information. Without the information, EAS cannot provide services.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use?

The only use of the information is to base services for the veterans. The information is not shared with anyone.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

Follow the format below:

Privacy Risk: The risk is that the notice is verbally provided at the time of the interview.

Mitigation: Veterans have access to this public PIA to see how their information is used.

http://www.oprm.va.gov/privacy/pia.aspx

Section 7: Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

During the initial interview process, validation of information is done as the veteran's record is added to EAS against what is recorded in the NPC. The veteran's PII must match before the EAS record can be saved. Any corrections to the NPC information must be done according the NPC SORN:

"National Patient Databases-VA" (121VA19) at http://www.gpo.gov/fdsys/pkg/FR-2010-11-26/pdf/2010-29695.pdf

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much.

Individuals wishing to obtain more information about access, redress, and record correction for the Environment Agents Service Registries should contact the Department of Veteran's Affairs regional office as directed in the System of Record Notices (SORNs) listed below:

"National Patient Databases-VA" (121VA19) at http://www.gpo.gov/fdsys/pkg/FR-2010-11-26/pdf/2010-29695.pdf

"Agent Orange Registry" (105VA131) at http://www.gpo.gov/fdsys/pkg/FR-2009-03-16/pdf/E9-5598.pdf

"Gulf War Registry" (93VA131) at http://www.gpo.gov/fdsys/pkg/FR-2015-03-03/pdf/2015-04313.pdf

"Ionizing Radiation Registry" 69VA131 at http://www.gpo.gov/fdsys/pkg/FR-2008-12-08/pdf/E8-29016.pdf

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.

Individuals seeking information regarding access to and contesting of VA records may write, call, or visit the nearest VA regional office. EAS SORNs are:

"National Patient Databases-VA" (121VA19) at http://www.gpo.gov/fdsys/pkg/FR-2010-11-26/pdf/2010-29695.pdf

"Agent Orange Registry" (105VA131) at http://www.gpo.gov/fdsys/pkg/FR-2009-03-16/pdf/E9-5598.pdf

"Gulf War Registry" (93VA131) at http://www.gpo.gov/fdsys/pkg/FR-2015-03-03/pdf/2015-04313.pdf

"Ionizing Radiation Registry" 69VA131 at http://www.gpo.gov/fdsys/pkg/FR-2008-12-08/pdf/E8-29016.pdf

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

Individuals seeking information regarding access to and contesting of VA records may write, call, or visit the nearest VA regional office. EAS SORNs are:

"National Patient Databases-VA" (121VA19) at http://www.gpo.gov/fdsys/pkg/FR-2010-11-26/pdf/2010-29695.pdf

"Agent Orange Registry" (105VA131) at http://www.gpo.gov/fdsys/pkg/FR-2009-03-16/pdf/E9-5598.pdf

"Gulf War Registry" (93VA131) at http://www.gpo.gov/fdsys/pkg/FR-2015-03-03/pdf/2015-04313.pdf

"Ionizing Radiation Registry" 69VA131 at http://www.gpo.gov/fdsys/pkg/FR-2008-12-08/pdf/E8-29016.pdf

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.

Consider the following FIPPs below to assist in providing a response:

Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

Follow the format below:

Privacy Risk: There is a risk that individuals may seek to access or redress records about them held by the VA and become frustrated with the results of their attempts.

Mitigation: By publishing this PIA and the applicable SORNs, the VA makes the public aware of the unique status of applications and evidence files. This document and the SORNs provide points of contact for members of the public who have questions or concerns about applications and evidence files.

Section 8: Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

Describe the process by which an individual receives access to the system.

Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system.

Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Per VA Directive and Handbook 6330, every 5 years the Office of Information & Technology (OI&T) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.

OI&T documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring is performed the Talent Management System (TMS).

8.2 Will VA contractors have access to the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required.

OI&T provides basic security awareness training to all information system users (including managers, senior executives, and contractors) of VA information systems or VA sensitive information as part of initial training for new users, when required by system changes and annually thereafter.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National RoB or VA Contractor's RoB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all

personnel must complete via the VA's TMS. After the user's initial acceptance of the RoB, the user must re-affirm their acceptance annually as part of the security training. Acceptance is obtained via electronic acknowledgement and is tracked through TMS.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

If so, provide the date the Authority to Operate (ATO) was granted. Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

Assessment and Accreditation (A&A) is in progress. An Authority to Operate with Conditions (ATOC) was granted on March 2, 2015 for 60 days.

Signature of Responsible Officials

The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

Tocilla, Artur (SMS)

Digitally signed by Tocilla, Artur (SMS)
DN: dc=gov, dc=va, ou=Entities, ou=InternalStaff, cn=Tocilla, Artur (SMS)
Date: 2015.06.17 11:22:44 -04'00'

Privacy Officer, Artur Tocilla or Mark Littlefield

Chan, Stephan

Digitally signed by Chan, Stephan
DN: dc=gov, dc=va, ou=Entities, ou=InternalStaff, cn=Chan, Stephan
Date: 2015.06.23 07:57:18 -04'00'

Information Security Officer, Stephan Chan

System Owner, Tammy Watson

Martha J. Clark 583966 (affiliate)

Digitally signed by Martha J. Clark 583966 (affiliate)
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=martha.clark4@va.gov, cn=Martha J. Clark 583966 (affiliate)
Date: 2015.06.23 12:10:01 -05'00'

Individual Completing the PIA, Martha Clark

Signature of Responsible Officials

The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

Tocilla, Artur (SMS)

Digitally signed by Tocilla, Artur (SMS)
DN: dc=gov, dc=va, ou=Entities, ou=InternalStaff, cn=Tocilla, Artur (SMS)
Date: 2015.06.17 11:22:19 -04'00'

_____

Privacy Officer, << INSERT NAME FROM COVER PAGE>>

_____

Information Security Officer, << INSERT NAME FROM COVER PAGE>>

Betty Heath _____

System Owner, << INSERT NAME FROM COVER PAGE>>

_____

Individual Completing the PIA, << INSERT NAME FROM COVER PAGE>>