

# Privacy Impact Assessment - 2009 (Form) / Automated Monument Application System (AMAS)-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:

Automated Monument Application System (AMAS)-2009

1.1.b) OMB Unique Project Identifier:

N/A

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.*

AMAS was developed by NCA FTE at the Quantico Regional Processing Center (QRPC) to automate all business processes associated monument ordering, delivering, and tracking. The intent was to automate all manual, paper-intensive record keeping, and information and forms processing associated with monument applications. AMAS receives, processes, and tracks over 330,000 applications for government-furnished monuments, i.e., headstones, markers, and niche covers each year. AMAS supports legislated benefits so its life cycle is indefinite. AMAS provides tracking capability for all claims entered in the system thus expediting case research and NCA's response to individual case inquiries. Demographic projections call for significant increases in workload over the next twenty years. In order to minimize increases in staff and operational expenditures during this time frame, and to maintain current levels of service, the NCA's Memorial Programs Service (MPS) is committed to automation at all levels of business operations. Through ongoing automation, integration, and standardization of AMAS functions, MPS will be able to accommodate an increasing workload, maximize the utilization of personnel and physical resources, and capture information needed for MPS and VA information resources management planning activities. NCA's Burial Operations Support System (BOSS) is closely aligned to the AMAS. Both are benefit delivery systems, and developed and maintained by NCA FTE. BOSS automates all manual, paper-intensive record keeping, and information and forms processing associated with interments. BOSS and AMAS share the same corporate database and some common tables. NCA continues to make technology refresh acquisitions, meet scheduled target dates, and meet or exceed performance goals. Our approach to technology refresh, migrations, and IT deployment is designed to ensure the highest return on investment and lowest cost of ownership. As part of VA's Capital Planning & Investment Control (CPIC) process, this investment was approved by the EIB on 5/25/2006.

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.*

#### 1.2) Contact Information:

<b>1.2.a) Person completing this document:</b>	
<b>Title:</b>	George Eisenbach
<b>Organization:</b>	Deputy Under Secretary for Memorial Affairs (41)
<b>Telephone Number:</b>	202-273-5153
<b>Email Address:</b>	George.Eisenbach@va.gov

<b>1.2.b) Project Manager:</b>	
<b>Title:</b>	Dennis Menor, Information Technology Specialist
<b>Organization:</b>	Applications Systems Division (41G2B)
<b>Telephone Number:</b>	703-441-3071
<b>Email Address:</b>	Dennis.Menor@va.gov
<b>1.2.c) Staff Contact Person:</b>	
<b>Title:</b>	William Barnes, Director
<b>Organization:</b>	Systems Integration Center (41G2)
<b>Telephone Number:</b>	703-441-2182
<b>Email Address:</b>	Bill.Barnes@cem.va.gov

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

## 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.)*

## 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 track applications for and delivery of Government-furnished headstones and markers; to locate burial locations of veterans interred in VA and Arlington National Cemeteries; and to obtain general information from records of interment.

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

AMAS supports legislative benefits outlined under: Title 38 Veterans' Benefits; Chapter 24 National Cemeteries and Memorials; Section 2402 Persons eligible for interment in national cemeteries.

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.

1,000,000 - 9,999,999

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.

(3) Operation/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.

The application has been operational since June, 1996.

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

#### 4. SYSTEM OF RECORDS:

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

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

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

Yes

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

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

Yes

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

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

AMAS: 48VA40B BOSS: 42VA41

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

AMAS: Veterans (Deceased) Headstone or Marker Records-VA  
BOSS: Veterans and Dependents National Cemetery Interment

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

The BOSS System of Record and AMAS System of Record can be accessed via the VA's intranet site:  
[http://vawww.va.gov/privacy/SystemsOfRecords/2001\\_Privacy\\_Act\\_GPO\\_SOR\\_compilation.pdf](http://vawww.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SOR_compilation.pdf)

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

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

Yes

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

Created specifically for this project

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

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

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

Modification of the System of Records is 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.*

*Explanation:*

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

**PIA SECTION 5**

**Project Name**

Automated Monument Application System (AMAS)-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	<b>Veteran's or Primary Subject's Personal Contact Information (name, address, telephone, etc.)</b>
-----	---

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

Information is collected to record the burial for historic purposes and provide eligibility for spouse's burial. Name, Address, Date of Birth, Date of Death, gender and SSN. The name and address of the next of kin are collected to facilitate any follow up with the family that might be necessary. Address of the Vet is collected to ensure NCA is providing service within 75 miles of 75% of the veteran population. Vet Gender is captured for statistical purposes. The SSN and Date of Birth (service and claim number may be collected as well) are collected for the Vet to assist with eligibility determination. Decedent Date of Death is collected because it is required for the marker.

Yes	<b>Other Personal Information of the Veteran or Primary Subject</b>
-----	---

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

Information is collected to record the burial for historic purposes and provide eligibility for spouse's burial. Name, Address, Date of Birth, Date of Death, gender and SSN. The name and address of the next of kin are collected to facilitate any follow up with the family that might be necessary. Address of the Vet is collected to ensure NCA is providing service within 75 miles of 75% of the veteran population. Vet Gender is captured for statistical purposes. The SSN and Date of Birth (service and claim number may be collected as well) are collected for the Vet to assist with eligibility determination. Decedent Date of Death is collected because it is required for the marker. The SSN is also collected for the person identified as being financially responsible for providing the private grave line so they may be reimbursed.

Yes	<b>Dependent Information</b>
-----	------------------------------

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

Information is collected to record the burial for historic purposes and provide eligibility for the burial. Name, Address, Date of Birth, Date of Death, gender and SSN are collected for the decedent and veteran. The name and address of the next of kin are collected to facilitate any follow up with the family that might be necessary. Address of the Vet is collected to ensure NCA is providing service within 75 miles of 75% of the veteran population. Vet Gender is captured for statistical purposes. The SSN and Date of Birth (service and claim number may be collected as well) are collected for the Vet to assist with eligibility determination. Decedent Date of Death is collected because it is required for the marker. The SSN is also collected for the person identified as being financially responsible for providing the private grave line so they may be reimbursed.

Yes	<b>Service Information</b>
-----	----------------------------

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

Information is collected to record the burial for historic purposes and provide eligibility for spouse's burial. The service and claim number may be collected for the Vet to assist with eligibility determination.

No	<b>Medical Information</b>
----	----------------------------

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

No	<b>Criminal Record Information</b>
----	------------------------------------

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

No	<b>Guardian Information</b>
----	-----------------------------

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

No	<b>Education Information</b>
----	------------------------------

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

No	Rehabilitation Information
----	----------------------------

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

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

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

BOSS/AMAS provides an electronic notification - First Notice of Death (FNOD) to VBA benefit systems: Compensation & Pension, Loan Guaranty, and Insurance & Education. FNOD contains privacy information needed for the sole purpose of identifying the deceased veteran, including social security number, claim number, and service number. VBA avoids paying millions of dollars in benefits to those no longer entitled according to federal regulation and speeds up processing of other benefits designed to help veteran families after the loss. FNOD serves to negate or reduce overpayments and subsequent collection activities.

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

## 5.2 Data Sources

Identify the source(s) of the collected information.

a) Select all applicable data source categories provided below.

b) For each category selected:

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

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

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

Yes	Veteran Source
-----	----------------

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

Eligibility Determination

Yes	<b>Public Source(s)</b>
-----	-------------------------

*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.*

Family will provide supporting information and documentation necessary for marker ordering.

Yes	<b>VA Files and Databases</b>
-----	-------------------------------

*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.*

BIRLS/IBBA is routinely used to verify eligibility.

Yes	<b>Other Federal Agency Source(s)</b>
-----	---------------------------------------

*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.*

The one outside source of information for NCA is the St. Louis Records Processing Center. Information is collected to determine eligibility.

Yes	<b>State Agency Source(s)</b>
-----	-------------------------------

*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.*

State Cemeteries (40) use the BOSS application to manage their interment activities and order headstones and markers. They collect the information from the families and funeral homes and enter it in BOSS. BOSS provides a repository for this data and facilitates the marker ordering process which takes place within AMAS. The States and VA can use this information for reports and planning purposes.

No	<b>Local Agency Source(s)</b>
----	-------------------------------

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

Yes	<b>Other Source(s)</b>
-----	------------------------

*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.*

Families, next-of-kin, friends of the deceased, and funeral directors are also sources of information. The Department of Army (Arlington National Cemetery) also is a source of information. Two DOD cemeteries, 36 state, military post, and interior cemeteries are also the source of information. The information is needed to determine eligibility.

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

**5.3 Collection Methods**

*Identify and describe how personal information is collected:*

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

No	<b>Web Forms:</b>	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	<b>Paper Forms:</b>	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.*

Paper Form VA 40-1330 Application for Standard Government Headstone or Marker for Installation in Private or State Veterans' Cemetery collects privacy information.

No	<b>Electronic File Transfer:</b>	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	<b>Computer Transfer Device:</b>	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	<b>Telephone Contact:</b>	Information is collected via telephone.
-----	---------------------------	---

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

Telephone media is used to collect or verify information when exception handling is performed in response to incomplete or inaccurate information furnished on the paper form VA 40-1330 Application for Standard Government Headstone or Marker for Installation in Private or State Veterans' Cemetery collects privacy information.

No	<b>Other Collection Method:</b>	Information is collected through a method other that those listed above.
----	---------------------------------	--

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

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

#### **5.4 Notice**

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

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

systems?

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?

Mandatory

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

The data collection is presented as being necessary to provide the marker.

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.)

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

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

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	<b>Web Forms:</b>
----	-------------------

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	<b>Paper Forms:</b>
-----	---------------------

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.

No	<b>Electronic File Transfer:</b>
----	----------------------------------

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	<b>Computer Transfer Device:</b>
----	----------------------------------

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	<b>Telephone:</b>
-----	-------------------

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.

NCA Notice 2006-06, October 13, 2006, Subject: Collection of PII to Determine Eligibility was disseminated to all Memorial Service Network Directors for distribution to their employees. Our employees continue to receive General Privacy training, to include new incoming employees.

No	<b>Other Method:</b>
----	----------------------

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.)

NCA Notice 2006-06, October 13, 2006, Subject: Collection of PII to Determine Eligibility was disseminated to all Memorial Service Network Directors for distribution to their employees. Our employees continue to receive General Privacy Training, to include new incoming employees.

### 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.

	<b>Web Forms:</b>
--	-------------------

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.

	<b>Paper Forms:</b>
--	---------------------

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.

	<b>Electronic File Transfer:</b>
--	----------------------------------

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.

	<b>Computer Transfer Device:</b>
--	----------------------------------

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.

	<b>Telephone Contact Media:</b>
--	---------------------------------

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.

There are no secondary uses of this data permitted, and as such, no consent is necessary because the information is used only to provide a benefit. For AMAS, the only information we collect on the VA Form 40-1330 that is considered protected would be the contact information (Applicant, Consignee, and Cemetery). The Applicant may or may not be the next of kin, it is usually who is filling out the form for the family or on their behalf. We do not require that it be submitted by the next of kin. These contact information are the name, mailing addresses, phone numbers, and sometimes a fax number or e-mail address. This information is only used by MPS to obtain additional information that might be needed to process the claim.

	<b>Other Media</b>
--	--------------------

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:

Functional requirements of the application were developed against NCA policy. The users are trained on the system. The system provides the necessary work flow process to limit the user to addressing only the necessary items.

5.6.b) *How is data checked for completeness?*

The system has edits and checks to verify entered data is not contradictory. The user is trained to also validate the information provided against system records or paper files.

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

The nature of the data makes it event specific and therefore it is to remain static.

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

The data related to eligibility must be validated against system records or paper files, i.e., DD214.

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


PIA SECTIONS 6 - 13

**Project Name**

Automated Monument Application System (AMAS)-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.

<input checked="" type="checkbox"/> Yes	<b>System Users</b>
---	---------------------

<input checked="" type="checkbox"/> Yes	<b>System Owner, Project Manager</b>
---	--------------------------------------

<input checked="" type="checkbox"/> Yes	<b>System Administrator</b>
---	-----------------------------

<input type="checkbox"/> No	<b>Contractor</b>
-----------------------------	-------------------

*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.*

<input checked="" type="checkbox"/> Yes	<b>Internal Sharing: Veteran Organization</b>
---	---

*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.*

VBA – Veteran Name, SSN, Address and Burial Location. Assists with the proper management of benefit delivery.

No	<b>Other Veteran Organization</b>
----	-----------------------------------

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

Yes	<b>Other Federal Government Agency</b>
-----	--

*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.*

Defense Manpower Data Center – Veteran Name, Address, SSN, Burial Location. Assists with the administration of their database and file maintenance.

No	<b>State Government Agency</b>
----	--------------------------------

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

No	<b>Local Government Agency</b>
----	--------------------------------

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

No	<b>Other Project/ System</b>
----	------------------------------

*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:

The system users at cemeteries have access to the personal information limited to what was entered by their facility. Except for the Veteran Information. That information is shared among all users.

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

Role of responsibility and location

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

Yes. Headstone and Marker applications – Privacy impact information is shared with veterans' families, funeral directors, and in-house personnel on a need-to-know basis. Gravesite Locator Information - Information is shared with the public to the extent that it is available on headstones or national cemetery kiosks. Next-of-kin information and social security numbers, and service numbers are not released to the public but at times are shared in-house on a need-to-know basis. Interment information – Privacy impact information is provided to the Department of Army's Defense Man-Power Data Center (DMDC) to facilitate updates to their database. Information that identifies the decedent and veteran is provided.

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

User access is restricted to the data of their facility and further limited by their position at the facility.

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)

All system users are must sign a rules of behavior and perform annual security training. Additionally, users are trained on the system by local staff. The system also has accounting and audit logs to provide reports on questionable activities.

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.

Privacy information is housed on a centralized database. Access is provided by user id and password. User access is tracked and all users must take annual privacy training.

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

The system owners of SHARE and BOSS/AMAS are responsible for ensuring their staffs and customers perform within VA's guidelines for protecting personal data per the inter system agreement. SHARE is a VBA application that has access to BOSS. The access is limited to a canned script that is initiated by the SHARE application to the BOSS database. The user provides the name and social to determine if a veteran has been interred.

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

Data is transmitted from system to system over the VA intranet and presented as part of the SHARE screen.

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.

Specific MOUs will be implemented by the end of the calendar year.

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

Users sign a Rules of Behavior document so that they understand their responsibilities to protect veteran data at all times

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

Currently we rely on their organizations to provide security and privacy training. That process will be formalized by the end of calendar year. The organization will have to show documented proof that they completed the VA General Privacy Training requirements.

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

## 6.2 Access to Records and Requests for Corrections

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

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

<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 type="checkbox"/>	The application will provide a phone number of a VA representative who will provide instructions.
<input checked="" 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?

They would have to request an information change. The public can only view the information made available through the Nationwide Grave Locator.

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

The customer requests to have information changed. If the request is valid, the change is made and the customer is notified.

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

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

We do not maintain official records. We maintain a copy of a request for a claim and any supporting documents to support the request (application and discharge papers). The application allows for the requestor (applicant) to submit a corrected copy if the first copy was submitted with errors. Our call center also receives calls when this happens, or someone needs to report an error or correction needed. This normally happens, for example, when an incorrect date of birth is provided on the first application, then a correction is submitted. We are not amending or changing any official record about the veteran.

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

## 7 Retention and Disposal

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

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

VA HBK 6300.1 Records Management Procedures explains the Records Control Schedule procedures.

**System of Records Notices may be accessed via:**

<http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm>

or

[http://vaww.va.gov/foia/err/enhanced/privacy\\_act/privacy\\_act.html](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](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](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.*

Data is housed on line. Data is retained permanently.

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

Per the System of Record, records can be retained and disposed of in accordance with disposition authorization approved by the Archivist of the United States. NCA has elected not to eliminate any data; data is retained permanently.

*7.c) Where are procedures documented?*

System of Record.

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

NCA has elected to retain records permanently.

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

Yes

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

NARA is only interested in the records when they are to be retired from the system.

## 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:

VA is constantly upgrading its security profile. Intrusion detection systems, virus updates, security patches, harden passwords, regular backups, etc.

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.

Information is secured and protected via computer logins and passwords. A password is required for access to the VA and NCA network. A separate password is required for access to the application. VA standards are followed for computer login and password establishment and maintenance; access to the network and applications are granted on a need-to-know basis. A FISMA survey was last completed in July 2004. A C&A was completed 10/1/2004. The Authorization to Operate (ATO) was granted July 11, 2005. National cemeteries physically secure all paper records that contain privacy impact information and follow directives and guidelines on their destruction, which includes burning and shredding. The computer room that houses the application is secured, only authorized personnel may enter. When appropriate information is to be released to the public, requests for such information are reviewed and information redacted, as needed, by NCA's FOIA/Privacy Officer. Social Security numbers and service numbers of the deceased are not released to the public nor is any information on the next-of-kin without their expressed permission.

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

Information is secured and protected via computer logins and passwords. A password is required for access to the VA and NCA network. A separate password is required for access to the application. VA standards are followed for computer login and password establishment and maintenance; access to the network and applications are granted on a need-to-know basis. A FISMA survey was last completed in July 2004. A C&A was completed 10/1/2004. The Authorization to Operate (ATO) was granted July 11, 2005. National cemeteries physically secure all paper records that contain privacy impact information and follow directives and guidelines on their destruction, which includes burning and shredding. When appropriate information is to be released to the public, requests for such information are reviewed and information

redacted, as needed, by NCA's FOIA/Privacy Officer. Social Security numbers and service numbers of the deceased are not released to the public nor is any information on the next-of-kin without their expressed permission.

**9. CHANGE RECORD**

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

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

No

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

--	--	--	--	--

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

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

<b>10. CHILDREN'S ONLINE PRIVACY PROTECTION ACT</b>
10.a) Will information be collected through the Internet from children under age 13?
No
If "No" then SKIP to Section 11, "PIA Considerations".
10.b) How will parental or guardian approval be obtained.
ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

<b>11. PIA CONSIDERATIONS</b>
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.
No changes were made to the IT system or collection of information after completing this PIA.
ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

<b>12. PUBLIC AVAILABILITY</b>
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 assessment <sup>9</sup> . 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.)

<b>13. ACCEPTANCE OF RESPONSIBILITY AND ACKNOWLEDGEMENT OF ACCOUNTABILITY:</b>
--

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)

Project Manager: Dennis Menor (5/18/2006) Owner: Joe Nosari (5/18/2006)

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