



PRIVACY IMPACT ASSESSMENT (PIA)

For the

ANC-ISS - ARLINGTON NATIONAL CEMETERY - INTERMENT SERVICES
SYSTEM

Arlington National Cemetery Provisional Oversight Group, OCIO

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- New DoD Information System
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR Enter DITPR System Identification Number
- Yes, SIPRNET Enter SIPRNET Identification Number
- No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes No
- If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- Yes No
- If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

Yes

Enter OMB Control Number

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

5 U.S.C. 301, Departmental Regulations
10 U.S.C. 3013, Secretary of the Army
Army Regulation 25-1, The Army Information Resources Management Program
AR 210-190, Post Cemeteries
DA Pamphlet 290-5, Administration, Operation, and Maintenance of Army Cemeteries
Executive Order 9397 (SSN), as amended.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

Arlington National Cemetery - Interment Services System (ANC-ISS) is an automated information system that supports Arlington National Cemetery with the scheduling of interments, management and accountability of burial records and coordination with the military services to provide honors associated with each service. System includes information on decedent data, eligibility data, funeral service data, interment data, and next of kin contact information. It is used by Arlington National Cemetery employees. Input - Decedent and interment information are manually inputted into the system by ANC. It is used by Arlington National Cemetery employees. This system can be used to populate DA 2122, JUN 82 Record of Interment/Inurnment.

PII collected includes personal information and military records.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Security risks inherent in maintaining data in an electronic environment have been mitigated using a variety of technical, physical, and administrative safeguards. Physical records are located within restricted areas accessible only to authorized ANC personnel. Physical access is controlled by multiple access controls: alarm system, surveillance system, properly cleared and trained personnel with approved need-to-know plus computer hardware and software security features. All PII is encrypted and accessible only by designated users with an assigned user role on a need-to-know basis. Safeguards employed are commensurate with the risk that would result from loss, misuse, unauthorized access or modification of the data.

PII RISK is associated as HIGH due to the number of records maintained within the system.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

Within the DoD Component.

Specify.

All Army components and major commands which includes active Army Accessions Command, Army Audit Agency, Army Cadet Command, Army Criminal Investigation Command, Army Deputy Chief of Staff for Personnel, Army G1, Army Inspectors General, Army Intelligence and Security Command, Army Recruiting Command, Army Recruiting Information Support System, Army Research Institute, Army Reserve Command and to Commanders of the Army Reserves, Army Training and Doctrine Command, Assistant Secretary of the Army (Financial Management & Comptroller), Department of the Army Inspectors General, Provost Marshal General, Army Staff Principals, within the chain of command, and supervisors and their designated human resources and administrative personnel responsible for processing personnel actions.

Other DoD Components.

Specify.

Defense Criminal Investigative Service, Defense Finance and Accounting Service, Defense Integrated Military Human Resources System, Defense Manpower Data Center, Defense Security Service, Department of Veterans Affairs, DoD Inspector General, Medical Command, National Guard Bureau,

Office of the DoD Inspector General, Office of the Secretary of Defense,
Office of the Secretary of Defense Personnel and Readiness, and U.S.
Military Entrance Processing Command.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

Contractor (Enter name and describe the language in the contract that safeguards PII.)

Specify.

NOTE: In discussions with Ms Reese from the Privacy Office the required FAR clauses listed below, will be incorporated into the new contracts which are to be recompeted in September 2015:

PRIVACY ACT NOTIFICATION (APR 1984)

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

PRIVACY ACT (APR 1984)

(a) The Contractor agrees to—

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies—

(i) The systems of records; and

(ii) The design, development, or operation work that the contractor is to perform;

(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

(3) Include this clause, including this paragraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.

(c)(1) "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

(2) "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

(3) "System of records on individuals," as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying

particular assigned to the individual.

-----Current Contract Language-----

The following contractors have access to the system: Booz Allen Hamilton; iBASEt; ArrowPoint, Lockheed MArtin, L3 Stratis and Excidion. Each contract has language similar to the content below.

1.6.7 Security Requirements:

1.6.7.1 The contractor is responsible for safeguarding information of a confidential or sensitive nature. Failure to safeguard any classified/privileged information which may involve the contractor or the contractor's personnel or to which they may have access may subject the contractor and/or the contractor's employees to criminal liability under Title 18, section 793 and 7908 of the United States Code. Provisions of the Privacy Act apply to all records and reports maintained by the contractor. All programs and materials developed at government expense during the course of this contract are the property of the government. At the time that the solicitation is issued, it should be accompanied by a Contract Security Specification, DD Form 254, in accordance with DoD Directive 5220.22-M, Department of Defense Industrial Security Manual for Safeguarding Classified Information, and any revisions, thereto, as well as Industrial Security Regulation DoD 5220.22-R. Failure to safeguard any classified/privileged information which may involve the contractor and/or the contractor's personnel or to which they may have access may subject the contractor and/or contractor's personnel to criminal liability under Title 18, section 793 and 7908 of the United States Code.

1.6.7.2 SecArmy memorandum dated 28 January 2006 on Contractor Verification System (CVS) Implementation provides guidance and instructions for the implementation of the CVS Army-wide. IAW that guidance, the authorizing official (Contracting Officer Representative (COR)), Contracting Officer Technical Representative (COTR), Contracting Officer, or other approving officials), the contractor's sponsor, approves issuance of the CAC through the automated CVS system. The COR in the BPA is the designated Trusted Agent (TA). Further delegation of that authority is determined at the installation level. The contractor's CVS applications under this task order should clearly cite the contract and task order numbers identified on the DD Form 1155 for this task order.

1.6.7.3 Physical Security. The contractor shall be responsible for safeguarding all government property provided for contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

Other (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

Yes

No

(1) If "Yes," describe method by which individuals can object to the collection of PII.

To determine eligibility, individuals consent to the capture and use of this information when requesting interment/inurnment at ANC. Without this consent, ANC cannot determine eligibility and therefore would not