DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office, Chief Information Officer / G-6

12 DEC 2006

SAIS-GKP

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Department of Army (DA) Privacy Impact Assessment (PIA) Guidance

1. References:

a. Memorandum, Office of Management and Budget (OMB), 26 September 2003, subject: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (url: http://whitehouse.gov/omb/memoranda/print/m03-22.html)

b. Memorandum, Department of Defense Chief Information Officer (CIO), 28 October 2005, subject: Department of Defense (DOD) Privacy Impact Assessment (PIA) Guidance (url: http://dod.mil/nii/pia/doc/DoD_PIA_Guidance_Oct_28_2005.pdf)

2. In accordance with requirements listed in paragraph 8.1. of reference b above, the CIO/G-6 is the Army PIA reviewing official. The PIA reviewing official will ensure that:

a. PIAs are conducted before developing or procuring information technology (IT) systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public (excluding DOD personnel), or initiating a new electronic collection of information in identifiable form for ten or more persons (excluding DOD personnel).

b. Supporting IT being developed and used protects and preserves the privacy of the American public.

c. The Army Portfolio Management Solution (APMS) includes data fields that identify IT systems or projects required to conduct PIAs.

3. References above provide policy on conducting PIA for IT systems that collect personal information on the public in order to ensure that handling of privacy information conforms to applicable legal, regulatory, and policy requirements. The DA supplement to the DOD policy is at enclosure 1. The PIA format is at enclosure 2. The definitions are at enclosure 3.

4. Owners of IT systems or projects are required to:

a. Conduct PIAs in accordance with the enclosed guidance to effectively address privacy factors for new or significantly altered IT systems or projects collecting information in identifiable form.

b. Report the requirement to conduct PIA in APMS.

5. This guidance applies to DA components, DA contractors, subcontractors, and entities developing or hosting information in electronic form for DA.

6. My point of contact for this action is Mr. Roy Baumann, comm: (703) 604-2018, DSN: 664-2018, e-mail: CIO/G6 PIA@hqda.army.mil.

3 Encls

for STEVEN W. BOUTELLE
Lieutenant General, GS
Chief Information Officer/G-6

DISTRIBUTION:
PRINCIPAL OFFICIALS OF HEADQUARTERS, DEPARTMENT OF ARMY

COMMANDER
US ARMY FORCES COMMAND
US ARMY TRAINING AND DOCTRINE COMMAND
US ARMY MATERIEL COMMAND
US ARMY EUROPE AND SEVENTH ARMY
US ARMY CENTRAL
US ARMY NORTH
US ARMY SOUTH
US ARMY PACIFIC
US ARMY SPECIAL OPERATIONS COMMAND
MILITARY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND
US ARMY SPACE AND MISSILE DEFENSE COMMAND/ARMY STRATEGIC COMMAND
EIGHTH US ARMY

CF:
COMMANDER
US ARMY NETWORK ENTERPRISE TECHNOLOGY COMMAND/9TH SIGNAL COMMAND
US ARMY MEDICAL COMMAND
(CONT)

DISTRIBUTION: (CONT)

US ARMY INTELLIGENCE AND SECURITY COMMAND
US ARMY CRIMINAL INVESTIGATION COMMAND
US ARMY CORPS OF ENGINEERS
US ARMY MILITARY DISTRICT OF WASHINGTON
US ARMY TEST AND EVALUATION COMMAND
US ARMY RESERVE COMMAND
US ARMY INSTALLATION MANAGEMENT COMMAND

SUPERINTENDENT, US MILITARY ACADEMY
DIRECTOR, US ARMY ACQUISTION SUPPORT CENTER

ARMY SUPPLEMENT TO

DOD PRIVACY IMPACT ASSESSMENT GUIDANCE

1. PURPOSE

1.1. Section 208 of the E-Government Act of 2002 establishes Government-wide requirements for conducting, reviewing, and publishing Privacy Impact Assessments (PIA). This guidance directs agencies to conduct reviews of how privacy issues are considered when purchasing or creating new Information Technology (IT) systems or when initiating new electronic collections of information in identifiable form. A PIA addresses privacy factors for all new or significantly altered Information Technology (IT systems or projects that collect, maintain, or disseminate personal information from or about members of the public - excluding information on DoD personnel.

2. APPLICABILITY AND SCOPE

2.1. This document applies to:

2.1.1. The Department of the Army (DA) staff, Army commands, and all other entities within DA (hereafter referred to collectively as the "DA").

2.1.2. DA contractors, vendors, or other entities that develop, procure, or use information technology systems under contract to DA, to collect, maintain, or disseminate information in identifiable form from or about members of the public.

3. POLICY

It is DA policy that:

3.1. The DA entities Components will adhere to the PIA requirements prescribed in the Office of Management and Budget's September 26, 2003, memorandum, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," and Department of Defense's October 28, 2005, memorandum, "Department of Defense (DOD) Privacy Impact Assessment (PIA) Guidance.

3.2. A Privacy Impact Assessment will be conducted before:

3.2.1. Developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public (excluding DoD personnel).

3.2.2. Initiating a new electronic collection of information in identifiable form for ten or more members of the public (excluding DoD personnel).

3.3. At the discretion of the DA entities, PIAs can be conducted on electronic collections and information systems containing information in identifiable form.

3.4. Although the PIA requirements may exclude DoD personnel, privacy implications should be considered for all systems and collections that involve information in identifiable form. When assessing the impact on privacy, DA Components will be guided by the privacy principles set forth in DoD Directive 5400.11, "DoD Privacy Program, "November 16, 2004 and AR 340-21, Army Privacy Program, July 8, 1985.

3.5 A PIA will be prepared using the format in Enclosure 2, by the DA Staff official or Army commander/director having responsibility for either procuring or developing the IT system or modifying an existing IT system to collect new information in identifiable form. Upon preparation, the PIA will be forwarded to the DA CIO/G-6 PIA Reviewing Official, which shall be the DA organization's CIO, who in consultation with both the DA organization's Information Assurance Official and the Privacy Officer, or their designees, shall review the PIA for approval. The DA CIO/G-6 Reviewing Official will ensure that the requirements set forth in the OMB guidance and this memorandum, have been addressed and that action is initiated when necessary, to correct any identified deficiencies. A reviewing official cannot be an official who is responsible for the development, procurement, or management of the system.

3.6. Army CIO/G-6 PIA reviewing official will maintain a repository of the PIAs. Army organizations will submit a electronic copy of the PIA to the following email address: CIO/G6 PIA@hqda.army.mil.

3.7. To facilitate public access, all approved PIAs shall be posted at a central location on the CIO/G-6 public website until the system is terminated, or the information in identifiable form is no longer housed on the system. The CIO/G-6 public website is http://www.army.mil/ciog6/links/privacyimpact.html. A "PIA Request" link will be maintained on the OASD(NII) website to respond to public requests regarding DoD IT systems containing information in identifiable form.

3.7.1 When publication of a PIA may raise security concerns (i.e., reveal classified or sensitive information), a summary of the PIA in a non-classified form is to be prepared, posted, and submitted. If a summary will not eliminate the security concerns, the PIA is not to be posted, but maintained by the Approving Official for

record and reporting purposes.

3.7.2 Posting of the full or summary PIAs, will only be done after OMB releases the President's Budget.

3.7.3 Posting of a PIA or a PIA summary shall be at the discretion of the Component CIO, in accordance with guidance herein, and in consultation with the Component Information Assurance Officials and Privacy Officers.

4. RESPONSIBILITIES

4.1. The Assistant Secretary of Defense for Networks and Information Integration/DoD CIO shall:

4.1.1. Serve as the DoD principal point of contact for IT matters relating to DoD PIAs.

4.1.2. Provide Department-wide guidance with respect to conducting, reviewing, and publishing of PIAs.

4.1.3. Maintain a Department public website that enables public access to approved PIAs or summary PIAs.

4.1.4. Collect and provide information, as necessary, to compile Congressional and OMB reports.

5.1. The Director of Administration and Management of the Office of the Secretary of Defense as the Senior Agency Official for Privacy shall:

5.1.1. Serve as the DoD principal point of contact for privacy policies.

5.1.2. Provide advice and assistance on privacy matters impacting DoD PIAs.

5.1.3. Maintain a Department public website that contains a link to Department PIA information.

5.1.4. The Chief of the Freedom of Information and Privacy Act Office, Office of the Administrative Assistant to the Secretary of the Army, will serve as the DA principal point of contact for privacy policies, provide advice and assistance on privacy matters impacting PIAs, and review all DA PIAs for privacy concerns.

6.1. The General Counsel of the Department of Defense shall provide advice and assistance on all legal matters arising out of, or incident to, the administration of PIAs.

6.1.1. Army organizations should consult their agency legal advisors for advice

and assistance on all legal matters arising out of, or incidental to, the administration of Army PIAs.

7.1. The Secretaries of the Military Departments and the Heads of the other DoD Components shall:

7.1.1. Establish necessary policies and procedures to implement guidance outlined in this memorandum; and educate employees and contractors on their responsibilities for protecting information in identifiable form that is being collected, maintained, or disseminated by IT systems.

8.1. HQDA Chief Information Officer/G-6 shall:

8.1.1. Serve as the DA PIA reviewing official.

8.1.2. Ensure that new or modified IT systems that collect, maintain, or disseminate information in identifiable form from or about members of the public, and/or new electronic collections of information in identifiable form for ten or more persons (excluding DoD personnel) have a PIA performed by the office responsible for the IT system or collection.

8.1.3. Ensure PIAs are completed before developing, procuring, or modifying the IT system; and acquire appropriate coordinations with the office submitting the request and the information assurance and privacy officials.

8.1.4. Forward to OMB, all PIAs for IT systems and projects, consistent with the OMB Circular A-11, Section 300.

8.1.5. Post approved PIAs, or summary PIAs, on the CIO/G-6 public website, and email the URL address to PIA@osd.mil for posting to the OASD(NII)/DoD CIO PIA web page. If a full or summary PIA does not meet the publishing requirements (see paragraph 3.7.), indicate on the public website the system name and note that the PIA is not publicly accessible.

8.1.6. Provide information to the DoD CIO, consistent with the guidance set forth in paragraph 4.1.4.

9.1. The HQDA Information Assurance official shall review and coordinate proposed PIAs to ensure compliance with DoD information assurance policies.

10.1. The HQDA Privacy Officer shall review and coordinate proposed PIAs to confirm that privacy implications have been identified and evaluated to ensure the proper balance is struck between an individual's personal privacy and DA's information

requirements.

ARMY SUPPLEMENT TO

DOD PRIVACY IMPACT ASSESSMENT (PIA) FORMAT

(Use N/A where appropriate)

1. Department of the Army organizational name (APMS Sub Organization name).

2. Name of Information Technology (IT) System (APMS System name).

3. Budget System Identification Number (SNAP-IT Initiative Number).

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)).

5. IT Investment (OMB Circular A-11) Unique Identifier (if applicable).

6. Privacy Act System of Records Notice Identifier (if applicable).

7. OMB Information Collection Requirement Number (if applicable) and Expiration Date.

8. Type of authority to collect information (statutory or otherwise).

9. Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup).

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g., names, Social Security Numbers, gender, race, other Army IT systems, other component IT systems, IT systems from agencies outside DoD, etc.).

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.).

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a DA program, etc.)

13. Describe how the information in identifiable form will be used (e.g., to verify existing data, etc.).

Fillable format is available at AKO:
https://www.us.army.mil/suite/folder/394537

14. Describe whether the system derives or creates new data about individuals through aggregation.

15. Describe with whom the information in identifiable form will be shared, both within DA and outside the DA (e.g., other Army organizations, other DoD Components, Federal agencies, etc.).

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.

17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory), as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program," November 16, 2004 and AR 340-21, Army Privacy Program, July 8, 1985. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur.

20. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.

Fillable format is available at AKO:
https://www.us.army.mil/suite/folder/394537

Preparing Official_____
Name
Title:
Organization:
Work Phone Number:
Email:
(signature)
(date)

Information Assurance Official_____
Name:
Title:
Organization:
Work Phone Number:
Email:
(signature)
(date)

Privacy Officer_____
Name:
Title:
Organization:
Work Phone Number:
Email:
(signature)
(date)

Reviewing Official_____
Name:
Chief Information Officer
Organization:
Work Phone Number:
Email:
(signature)
(date)

Fillable format is available at AKO:
https://www.us.army.mil/suite/folder/394537

DEFINITIONS

In addition or in lieu of the terms defined in Part II.A. of the OMB Guidance, the following definitions apply:

- "DA Personnel" includes:

  Members of the Armed Forces (to include Reserve and National Guard personnel) and DA civilian employees (including non-appropriated fund employees). DA contractors, vendors, or other entities that develop, procure, or use information technology systems under contract to DA, to collect, maintain, or disseminate information in identifiable form from or about members of the public.

- "Information Technology" (IT) is any equipment or interconnected system or
  subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Executive Agency. This includes equipment used by DA entities directly or used by a contractor under a contract with the Component that:

  Requires the use of such equipment; or

  Requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

- "Information in Identifiable form" is information in an IT system or online collection: (1) that directly identifies an individual (e.g., name, address, Social Security Number or other identifying number or code, telephone number, email address, etc.) or (2) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

- "National Security Systems" – means, as defined in the Clinger-Cohen Act, an information system operated by the federal government, the function, operation or use of which involves: (a) intelligence activities, (b) cryptologic activities

related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons systems, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management.

- Privacy Impact Assessment (PIA) – is an analysis of how information is handled: (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (2) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.