DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

16 June 2006

MEMORANDUM FOR DISTRIBUTION

Subj: DEPARTMENT OF DEFENSE AND DEPARTMENT OF THE NAVY PRIVACY IMPACT ASSESSMENT GUIDANCE

Ref: (a) The E-Government Act of 2002 (PL 107-347)
(b) Office of Management and Budget Memorandum 03-22 of 26 September 2003, "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002" (26 September 2003)
(c) SECNAVINST 5211.5E, "The Department of the Navy Privacy Program"

Encl: (1) Department of Defense Chief Information Office Memorandum of 28 October 2005, " Department of Defense Privacy Impact Assessment Guidance"

Protecting the privacy of Sailors, Marines, civilians, and members of the public is vitally important to the Department of the Navy (DON). Appropriately safeguarding personal information is crucial in order to avoid identity theft and maintain the security of our personnel and information systems. To that end, privacy requirements and specifications must be addressed when information technology (IT) systems that contain information in identifiable form (IIF) are being developed, procured, modified or used. IIF is defined as information in an IT system or online collection that directly identifies an individual (e.g., name, address, social security number or other identifying code, telephone number, email address, etc) or by which an agency intends to identify specific individuals in conjunction with other data elements (i.e., indirect identification that may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

Enclosure (1) requires that all Department of Defense (DoD) components, contractors, and entities developing or hosting information in electronic form for the DoD conduct Privacy Impact Assessments (PIAs) as per references (a) and (b). The PIA is the tool for assessing privacy risks in an information system. Federal and DoD guidance regarding PIAs helps ensure that IIF in electronic form is only acquired and maintained when necessary, and that the supporting IT systems being developed and used protect and preserve the privacy of the American public.

Accordingly, all DON activities are required to perform PIAs to effectively address privacy factors for new or significantly altered IT systems or projects collecting IIF from or about members of the public and DON civilian and military personnel. By extending the PIA requirement beyond the Federal and DoD requirement to include systems with IIF solely from or about DON personnel, the DON demonstrates its commitment to supporting the warfighter in every aspect of its operations. Privacy Impact Assessments must be conducted using the prescribed DoD format as provided in the attached enclosure. Privacy impact assessments will be performed by the DON official responsible for procuring or developing the IT system or modifying an existing system to collect new IIF.

Subj: DEPARTMENT OF DEFENSE AND DEPARTMENT OF THE NAVY PRIVACY IMPACT ASSESSMENT GUIDANCE

The Department of the Navy Chief Information Officer, as the DON PIA Reviewing Official, is responsible for:

1. Reviewing and approving PIAs to ensure that the requirements of references, (a), (b), and (c) have been met;
2. Ensuring remedial action is being taken against any privacy deficiencies identified in PIAs; and
3. Submitting approved PIAs to DoD and to the Office of Management and Budget according to Federal and DoD guidelines.

Further policy guidance on the responsibilities of DON personnel regarding PIAs can be found in reference (c). The required DoD PIA format and additional DON PIA guidance are available at http://www.doncio.navy.mil.

Protection of personal information is vital to our mission. We must all be mindful of the goal of protecting the privacy of the individual as we transform the DON into a secure, interoperable, net-centric naval information management/IT enterprise.

The DON CIO team is available to answer questions on PIAs. The point of contact for PIAs is Darin Dropinski, at 703-601-0120.

D. M. Wennergren

Distribution:
Immediate Office of the Secretary (ASN(M&RA), ASN(RD&A), ASN(I&E), ASN(FM&C), AAUSN)
Dept of the Navy Staff Offices (OPA, JAG, OLA, CHINFO, AUDGEN, CNR, NAVINSGEN)
GC
CNO (N09B, N091, N093, N095, N096, N097, N098, N1, N2, N3/5, N4, N6/N7, N8)
CMC (ARI, M&RA, I, I&L, PP&O, C4, P&R)
COMFLTFORCOM
COMPACFLT
COMUSNAVEUR
COMNAVSEASYSCOM
CHNAVPERS
COMSC
OPNAVSUPPACT
FLDSUPPACT
USNA

Distribution: (continued)
COMUSNAVCENT
COMNAVRESFORCOM
COMNAVAIRSYSCOM
BUMED
NETC
COMSPAWARSYSCOM
COMNAVSUPSYSCOM
DIRSSP
CNI
PRESINSURV
COMNAVLEGSVCCOM
ONI
COMNAVSAFECEN
COMNAVFACENGCOM
NAVSTKAIRWARCEN
COMNAVSECGRU
COMNAVDIST
NAVPGSCOL
NAVWARCOL
COMNAVSPECWARCOM
NAVHISTCEN
COMNAVNETWARCOM
PEO (Aircraft Carriers)
PEO (Air, ASW, Assault & Special Mission Programs)
PEO (Strike Weapons and Unmanned Aviation)
PEO (Joint Strike Fighter)
PEO (Integrated Warfare)
PEO (Ships)
PEO (Submarines)
PEO (Littoral and Mine Warfare)
PEO (Tactical Air Programs)
PEO (C4I and Space)
PEO (Space Systems)
PEO (Enterprise Information Systems)
DRPM (Strategic Systems Programs)
DRPM (Expeditionary Fighting Vehicle)
DRPM (Enterprise Resource Planning)
DRPM (NMCI)
DRPM (DCGSN)

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

October 28, 2005

CHIEF INFORMATION OFFICER

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Department of Defense (DoD) Privacy Impact Assessment (PIA) Guidance

This memorandum and its attachments (DoD Guidance, DoD PIA Format, and Definitions), provide Department-wide guidance to implement the PIA requirements mandated in Section 208 of the Electronic Government Act of 2002. The DoD Components will adhere to the PIA requirements prescribed in the Office of Management and Budget's (OMB) September 26, 2003, memorandum, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," in addition to the DoD-specific requirements outlined in this memorandum. OMB's guidance can be found at www.whitehouse.gov/omb/memoranda/m03-22.

The goal of the Department is to ensure personal information in electronic form is only acquired and maintained when necessary, and that the supporting information technology that is being developed and used protects and preserves the privacy of the American public. Accordingly, addressees are required to 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.

This guidance applies to DoD Components, DoD contractors, and entities developing or hosting information in electronic form for the Department. The point of contact for DoD PIAs is Megen Davis, who can be reached at Megen.Davis@osd.mil.

for Priscilla E. Guthrie
Deputy Assistant Secretary of Defense
(Deputy CIO)

Attachments

ATTACHMENT 1

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 Office of the Secretary of Defense (OSD), Military Departments, Chairman of the Joint Chiefs of Staff, Combatant Commands, Defense Agencies, DoD Field Activities, and all other entities within DoD (hereafter referred to collectively as the "DoD Components").

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

3. POLICY

It is DoD policy that:

3.1. The DoD 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," in addition to the DoD-specific requirements outlined in this memorandum. Component specific guidance will be consistent with the policy and requirements herein.

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 DoD Component, PIAs can be conducted on electronic collections and information systems containing information in identifiable form on DoD personnel.

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, Components will be guided by the privacy principles set forth in DoD Directive 5400.11, "DoD Privacy Program," November 11, 2004.

3.5. A PIA will be prepared using the format in Attachment 2, by the Component official 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 DoD Component Reviewing Official, which shall be the Component CIO, who in consultation with both the Component Information Assurance Official and the Privacy Officer, or their designees, shall review the PIA for approval. The 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. Each DoD Component will maintain a repository of the PIAs. Also, DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at pia@osd.mil and to OMB, consistent with the OMB Circular A-11, Section 300.

3.7. To facilitate public access, all approved PIAs shall be posted at a central location on the Component's public website until the system is terminated, or the information in identifiable form is no longer housed on the system. 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.

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.

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. The Component Chief Information Officers shall:

8.1.1. Serve as the Component 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 Component's 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 Component Information Assurance official shall review and coordinate proposed PIAs to ensure compliance with DoD information assurance policies.

10.1. The Component 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 the Component's information requirements.

ATTACHMENT 2

DOD PRIVACY IMPACT ASSESSMENT (PIA) FORMAT

(Use N/A where appropriate)

1. Department of Defense (DoD) Component.

2. Name of Information Technology (IT) System.

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 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 Component program, etc.)

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

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 the Component and outside the Component (e.g., 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 11, 2004. 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.

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

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

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

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

ATTACHMENT 3

DEFINITIONS

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

- "DoD Personnel" includes:

  Members of the Armed Forces (to include Reserve and National Guard personnel) and DoD civilian employees (including non-appropriated fund employees).

- "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 a Component 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.