



Department of Defense INSTRUCTION

NUMBER 5400.16
February 12, 2009

ASD(NII)/DoD CIO

SUBJECT: DoD Privacy Impact Assessment (PIA) Guidance

References: See Enclosure 1

1. PURPOSE. This Instruction:

a. Establishes policy and assigns responsibilities for completion and approval of PIAs in accordance with the guidance in DoD Instruction 5025.01 (Reference (a)) and the authority in DoD Directive 5144.1 (Reference (b)).

b. Provides procedures for the completion and approval of PIAs in the Department of Defense to meet the statutory requirement as stated in section 208 of Public Law 107-347 (Reference (c)) to analyze and ensure personally identifiable information (PII) in electronic form is collected, stored, protected, used, shared, and managed in a manner that protects privacy. These procedures also support Office of Management and Budget (OMB) Memorandum M-03-22 (Reference (d)).

c. Supersedes DoD Deputy Chief Information Officer (CIO) Memorandum (Reference (e)).

2. APPLICABILITY AND SCOPE. This Instruction applies to:

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

b. DoD information systems and electronic collections including those supported through contracts with external sources that collect, maintain, use, or disseminate PII about members of the public, Federal personnel, contractors, or in some cases foreign nationals.

3. DEFINITIONS. Unless otherwise noted, these terms and their definitions are for the purpose of this Instruction.

- a. DoD Information System. Defined in DoDD 8500.01E (Reference (f)).
- b. electronic collection. Any collection of information enabled by information technology.
- c. Federal personnel. Defined in DoD 5400.11-R (Reference (g)).
- d. National Security System. Defined in subchapter III of chapter 35 of title 44, U.S.C. (Reference (h)).
- e. PII. Defined in DoDD 5400.11 (Reference (i)).
- f. PIA. Defined in Reference (d).

4. POLICY. It is DoD policy that:

a. PIAs are completed on DoD information systems and electronic collections that collect, maintain, use, or disseminate PII in order to:

- (1) Ensure PII handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- (2) Determine the need, privacy risks, and effects of collecting, maintaining, using, and disseminating PII in electronic form; and
- (3) Examine and evaluate protections and alternative processes to mitigate potential privacy risks.

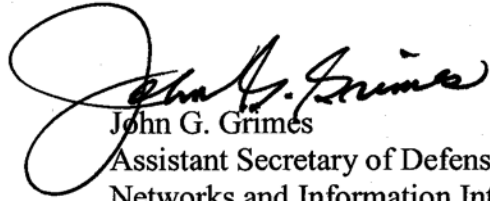
b. PIAs are performed when PII about members of the public (Reference (c)), Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally, is collected, maintained, used, or disseminated in electronic form.

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Issuances Web Site at <http://www.dtic.mil/whs/directives>.

8. EFFECTIVE DATE. This Instruction is effective immediately.



John G. Grimes
Assistant Secretary of Defense for
Networks and Information Integration/
DoD Chief Information Officer

Enclosures

1. References
2. Responsibilities
3. Procedures

TABLE OF CONTENTS

REFERENCES5

RESPONSIBILITIES6

 ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION
 INTEGRATION/DoD CHIEF INFORMATION OFFICER (ASD(NII)/DoD CIO)6

 DIRECTOR OF ADMINISTRATION AND MANAGEMENT (DA&M)6

 GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE6

 HEADS OF THE DoD COMPONENTS6

 DoD COMPONENT CIOs7

PROCEDURES8

 DETERMINATION OF NEED8

 PIA COMPLETION AND APPROVAL9

 PUBLISHING10

 SUBMISSION10

 REVIEW AND UPDATE CYCLE10

ENCLOSURE 1

REFERENCES

- (a) DoD Instruction 5025.01, "DoD Directives Program," October 28, 2007
- (b) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
- (c) Section 208 of Public Law 107-347, "E-Government Act of 2002," December 17, 2002
- (d) Office of Management and Budget (OMB) Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," September 26, 2003
- (e) DoD Deputy Chief Information Officer Memorandum, "Department of Defense (DoD) Privacy Impact Assessment (PIA) Guidance," October 28, 2005 (hereby canceled)
- (f) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
- (g) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
- (h) Subchapter III of Chapter 35 of title 44, United States Code
- (i) DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007
- (j) Sections 552 and 552a of title 5, United States Code
- (k) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007

ENCLOSURE 2

RESPONSIBILITIES

1. ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DoD CHIEF INFORMATION OFFICER (ASD(NII)/DoD CIO). The ASD(NII)/DoD CIO shall:

- a. Serve as the DoD principal point of contact for IT matters relating to DoD PIAs.
- b. Provide Department-wide guidance with respect to conducting, reviewing, and publishing PIAs.
- c. Maintain a DoD Web site that enables public access to approved PIAs or summary PIAs.
- d. Collect and provide pertinent information to compile Congressional and OMB reports.
- e. Report PIA statistical information to the DoD Senior Agency Official for Privacy for inclusion in the annual report to OMB.
- f. Submit DoD Component Chief Information Officer (CIO)-approved PIAs to OMB, as required.

2. DIRECTOR OF ADMINISTRATION AND MANAGEMENT (DA&M). As the senior agency official for privacy, in accordance with Reference (i), the DA&M shall:

- a. Serve as the DoD principal point of contact for privacy policies.
- b. Provide advice and assistance on privacy matters impacting DoD PIAs.
- c. Maintain a DoD public Web site that contains a link to ASD(NII)/DoD CIO PIA information.

3. GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE. 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.

4. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

- a. Ensure the DoD Component CIOs and Privacy Officials comply with this Instruction.
- b. Establish necessary policies and procedures to implement this Instruction.

c. Ensure the DoD Components adhere to the PIA requirements prescribed in References (c) and (d) and the DoD-specific requirements in this Instruction.

d. Minimize the collection and use of PII to the extent practicable as set forth in Reference (i).

5. DoD COMPONENT CIOs. The DoD Component CIOs shall:

a. Serve as the DoD Component PIA review and approval official.

b. Ensure that DoD information systems and electronic collections that collect, maintain, use, or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally, have a PIA completed by the office responsible for the DoD information system or electronic collection.

c. Ensure PIAs are completed according to the guidance provided in this Instruction.

d. Ensure PIA coordination between the office submitting the PIA request and Component information assurance and privacy officials.

e. Forward electronic copies of PIAs to the DoD CIO at pia@osd.mil. DoD Components will no longer submit PIAs directly to OMB. PIAs required to be submitted to OMB will be forwarded by ASD(NII)/DoD CIO.

f. Post approved PIAs, DD Form 2930, Sections 1 and 2 only, on the DoD Component's public Web site and e-mail the URL address to pia@osd.mil.

g. Within 120 days of the effective date of this Instruction, submit DoD Component CIOs' PIA implementation guidance to the OASD(NII)/DoD CIO for approval if different from this guidance.

ENCLOSURE 3

PROCEDURES

1. DETERMINATION OF NEED. The Program Manager or designee will review the DoD information system or electronic collection to determine if PII is collected, maintained, used, or disseminated about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally.

a. A PIA is not required if:

(1) No PII is collected.

(2) The information system is a National Security System in accordance with References (c) and (d). Although the PIA requirements exclude National Security Systems, privacy implications are to be considered for all DoD information systems and electronic collections that collect PII. When assessing the impact on privacy, DoD Components will be guided by the privacy principles set forth in References (g) and (i).

b. If PII is collected, a PIA or updated PIA is required for the following conditions:

(1) For existing DoD information systems and electronic collections for which a PIA has not previously been completed, including systems that collect PII about Federal personnel and contractors.

(2) In accordance with Reference (d), for new information systems or electronic collections:

(a) Prior to developing or purchasing new information systems or electronic collections;

(b) When converting paper-based records to electronic systems; or,

(c) When functions applied to an existing information collection change anonymous information into PII.

(3) For DoD information systems or electronic collections with a completed PIA, when change creates new privacy risks including the examples stated in subparagraphs 1.b.(3)(a) through 1.b.(3)(f).

(a) Significant System Management Changes. When new uses of an existing IT system, including application of new technologies, significantly change how PII 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.

(b) Significant Merging. When agencies adopt or alter business processes so that government databases holding PII 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.

(c) 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.

(d) Commercial Sources. When agencies systematically incorporate into existing IT systems databases of PII 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.

(e) New Interagency Uses. When Federal agencies work together on shared functions involving significant new uses or exchanges of PII, such as the cross-cutting E-Government initiatives.

(f) Alteration in Character of Data. When new PII added to a collection raises the risks to personal privacy (e.g., the addition of health or financial information).

c. No PIA is required where information relates to internal Government operations, when information has been previously assessed under an evaluation similar to a PIA (e.g., data use agreement), where privacy issues are unchanged from a previous assessment of PII, or as stated in subparagraphs 1.c.(1) through 1.c.(3) below, in accordance with Reference (d).

(1) For Government-run public Web sites where the user is given the option of contacting the site operator for the limited purposes of providing feedback (e.g., questions or comments) or obtaining additional information;

(2) When all elements of a PIA are addressed in a matching agreement governed by the computer matching provisions of the Privacy Act of 1974 (sections 552a(a)(8-10), (e)(12), (o), (p), (q), (r), and (u) of title 5, United States Code (Reference (j))), which specifically provides privacy protection for matched information; and

(3) When all elements of a PIA are addressed in an interagency agreement permitting the merging of data for strictly statistical purposes and where the resulting data are protected from improper disclosure and use.

2. PIA COMPLETION AND APPROVAL

a. The PIA will be prepared using DD Form 2930, "Privacy Impact Assessment (PIA)" available on the Internet from the DoD Forms Management Web Site at <http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm>.

b. Completion of the PIA requires coordination by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

c. The DoD Component Senior Information Assurance Officer shall review completed PIAs and confirm compliance with DoD information assurance policies, to include, if required, that the "Privacy Impact Assessment Required" data element is appropriately documented in System Identification Profiles in accordance with DoD Instruction 8510.01 (Reference (k)).

d. The DoD Component Privacy Officer shall review completed PIAs and confirm compliance with References (g) and (i).

e. The DoD Component CIOs shall serve as the DoD Component PIA final review and approval official.

3. PUBLISHING

a. Each DoD Component will maintain a central repository of its PIAs on the Component's public Web site until PII is no longer maintained in the system or the system is not in operation.

b. Publish only Sections 1 and 2 of DD Form 2930.

c. If Sections 1 and 2 of DD Form 2930 contain information that would raise security concerns or reveal classified or sensitive information, the DoD Component can restrict the publication of the assessment. Such information shall be protected and handled consistent with the Freedom of Information Act, section 552 of Reference (j).

d. The DoD CIO PIA Web site will be the central link to the Component PIA Web sites.

4. SUBMISSION. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at pia@osd.mil.

5. REVIEW AND UPDATE CYCLE

a. Review and update of existing PIAs for DoD information systems must be synchronized with the information system's certification and accreditation (C&A) cycle.

b. Review and update of existing PIAs for electronic collections must be completed within 3 years of PIA approval date.

c. Review and update of a PIA is required when a significant system change or a change in privacy or security posture occurs.