# Department of Defense
# INSTRUCTION

**NUMBER** 5400.16
July 14, 2015

DoD CIO

SUBJECT: DoD Privacy Impact Assessment (PIA) Guidance

References: See Enclosure 1

1. PURPOSE. This instruction:

a. In accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (a)), reissues DoD Instruction 5400.16 (Reference (b)) to establish policy and assign responsibilities for completion and approval of PIAs.

b. Provides procedures for the completion and approval of PIAs in DoD 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)).

2. APPLICABILITY. This instruction applies to 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 DoD (referred to collectively in this instruction as the "DoD Components").

3. POLICY. It is DoD policy that PIAs are:

a. Completed on DoD Information Technology (IT) and electronic collections that collect, maintain, use, or disseminate PII 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.

(3) Examine and evaluate protections and alternative processes to mitigate potential privacy risks.

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

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

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. RELEASABILITY. **Cleared for public release**. This instruction is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE. This instruction is effective July 14, 2015.

Terry A. Halvorsen
Department of Defense
Chief Information Officer

Enclosures
1. References
2. Responsibilities
3. Procedures

Glossary

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014
(b) DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," February 12, 2009 (hereby canceled)
(c) Section 208 of Public Law 107-347, "E-Government Act of 2002," December 17, 2002
(d) Office of Management and Budget Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," September 26, 2003
(e) DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014
(f) Office of Management and Budget Memorandum M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications," June 25, 2010
(g) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
(h) Title 5, United States Code
(i) DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015
(j) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(k) Committee on National Security Systems Instruction Number 4009, "National Information Assurance (IA) Glossary," current edition

ENCLOSURE 2

RESPONSIBILITIES

1. DOD CHIEF INFORMATION OFFICER (DOD CIO). The DoD CIO:

a. Serves as the DoD principal point of contact for IT matters relating to DoD PIAs.

b. Establishes policy and provides DoD-wide guidance with respect to conducting, reviewing, and publishing PIAs.

c. Maintains a DoD website that enables public access to approved PIAs or summary PIAs.

d. Collects and provides pertinent information to compile congressional and OMB reports.

e. Reports PIA statistical information to the DoD senior agency official for privacy for inclusion in the annual report to OMB.

f. Submits DoD CIO approved PIAs to OMB, as required.

2. DEPUTY CHIEF MANAGEMENT OFFICER (DCMO). As the senior agency official for privacy, in accordance with DoDD 5400.11 (Reference (e)), the DCMO:

a. Serves as the DoD principal point of contact for privacy policies.

b. Provides advice and assistance on privacy matters impacting DoD PIAs.

c. Maintains a DoD privacy public website that contains a link to DoD CIO PIA information.

3. GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE. The General Counsel of the Department of Defense will provide advice and assistance on all legal matters arising out of, or incident to, the administration of PIAs.

4. DOD COMPONENT HEADS. The DoD Component heads:

a. Ensure the DoD Component chief information officers (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 out in Reference (e).

e. Oversee the DoD Component CIOs. The DoD Component CIOs:

(1) Serve as the DoD Component PIA approval officials.

(2) Ensure PIAs are completed according to the guidance provided in this instruction.

(3) Ensure PIA coordination between the office submitting the PIA request and DoD Component cybersecurity and privacy officials.

# ENCLOSURE 3

# PROCEDURES

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

a. If PII is collected, a PIA is required for:

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

(2) In accordance with Reference (d), new IT, or electronic collections:

(a) Before developing, purchasing, or contracting new information systems or electronic collections;

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

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

(3) DoD IT or electronic collections with a completed PIA, when change creates new privacy risks, including the examples stated in paragraphs 1a(3)(a) through 1a(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).

b. An adapted PIA is required by the OMB in accordance with OMB Memorandum M-10-23 (Reference (f)) when a DoD Component's use of a third-party website or application may make PII available to the DoD Component.

c. A PIA is not required if:

(1) No PII is collected.

(2) The IT is a National Security System in accordance with Reference (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 out in Reference (e) and DoD 5400.11-R (Reference (g))

d. No PIA is required where information relates to internal U.S. 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 paragraphs 1d(1) through 1d(3) of this section, in accordance with Reference (d).

(1) For U.S. Government-run public websites where the user is given the option of contacting the site operator for the limited purpose 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 sections 552a(a)(8-10), (e)(12), (o), (p), (q), (r), and (u) of Title 5, United States Code, also known as the Privacy Act of 1974 (Reference (h)), which specifically provides privacy protection for matched information.

(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 Website at http://www.dtic.mil/whs/directives/infomgt/forms/index.htm. The DD Form 2930A, "Adapted Privacy Impact Assessment (PIA)," is used in accordance with Reference (f).

b. Completion of the PIA requires coordination by the program manager or designee through the information system security manager and privacy representative at the local level. Coordinate with the applicable records management office to ensure appropriate lifecycle management of any records created are maintained, used, preserved, and disposed of in accordance with DoD Instruction 5015.02 (Reference (i)) and National Archives and Records Administration approved records schedules.

c. The DoD Component senior information security officer will review completed PIAs and confirm compliance with DoD cybersecurity policies.

d. The DoD Component privacy officer will review completed PIAs and confirm compliance with Reference (e).

e. The DoD Component CIOs will 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 website 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 will be protected and handled consistent with section 552 of Reference (h), also known as the Freedom of Information Act.

d. The DoD CIO PIA Website will be the central link to the DoD Component PIA websites. If the component PIA Website changes, the component PIA representative will send an updated URL to osd.mc-alex.dod-cio.mbx.pia@mail.mil.

4. SUBMISSION. DoD Components submit an electronic copy of each approved PIA to the osd.mc-alex.dod-cio.mbx.pia@mail.mil. The appointed DoD CIO PIA action officer forwards only the public required PIAs to OMB.

5. REVIEW AND UPDATE CYCLE. Review and update of existing PIAs:

a. For DoD IT must be synchronized with the information system's assessment and authorization cycle.

b. For electronic collections must be completed within 3 years of PIA approval date.

c. Is required when a significant system change or a change in privacy or security posture occurs.

# GLOSSARY

## PART I. ABBREVIATIONS AND ACRONYMS

| | |
|---|---|
| CIO | Chief Information Officer |
| DCMO | Deputy Chief Management Officer |
| DD | Department of Defense (Form) |
| DoD CIO | Department of Defense Chief Information Officer |
| DoDD | Department of Defense directive |
| E-Government | Electronic Government |
| IT | Information Technology |
| OMB | Office of Management and Budget |
| PIA | Privacy Impact Assessment |
| PII | personally identifiable information |

## PART II. DEFINITIONS

These terms and their definitions are for the purposes of this instruction.

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).

commercial sources. When agencies systematically incorporate into existing IT systems databases of PII purchased or obtained from commercial or public sources.

E-Government initiatives. The use of information and communication technologies to improve the activities of public sector organizations.

DoD information system. Defined in DoD Instruction 8500.01 (Reference (j)).

DoD IT. Defined in Reference (j).

DoD personnel. Defined in Reference (e).

electronic collection. Any collection of information enabled by information technology.

National Security System. Defined in Committee on National Security Systems Instruction Number 4009 (Reference (k)).

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.

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.

PII. Defined in Reference (e).

records management. Defined in Reference (i).

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.

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.