



Office, Chief Information Officer/G-6

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

SAIS-CBA

OCT 25 2013

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Guidance for Submission of Privacy Impact Assessments (PIAs)

1. References:

- a. Army Regulation 25-1, Army Information Technology, 25 Jun 13.
 - b. Department of the Army Pamphlet 25-1-1, Army Information Technology Implementation Instructions, 25 Jun 13.
 - c. Section 208 of the E-Government Act of 2002, Pub. L. 107-347.
 - d. Department of Defense (DoD) Directive 5400.11, DoD Privacy Program, 8 May 07.
 - e. DoD 5400.11-R. DoD Privacy Program, 14 May 07.
 - f. DoD Instruction 5400.16, Privacy Impact Assessment (PIA) Guidance, 12 Feb 09.
 - g. Department of the Army (DA) Updated Guidance for Submission of Privacy Impact Assessment (PIA), 31 Jul 09 (hereby canceled).
2. This memorandum supplements AR 25-1 requirements for the submission of Privacy Impact Assessments for the Army and defines the term data collection instrument (DCI).
3. A PIA is an analysis of how Personally Identifiable Information (PII) is handled in electronic form by DCIs. (For examples of PII, see paragraph 1 of the enclosure.)
- a. A PIA determines the risks and effects of DCIs' collecting, maintaining and disseminating information in identifiable electronic form. (For examples of DCIs, see paragraph 2 of the enclosure.)
 - b. A PIA examines and evaluates protection and alternative processes for handling information to mitigate potential privacy risks.

SAIS-CBA

SUBJECT: Guidance for Submission of Privacy Impact Assessments (PIAs)

c. A PIA conforms to applicable legal, regulatory and policy requirements regarding privacy.

4. If a DCI has the ability to retrieve an individual's name, date of birth, social security number and contains a personal identifier of an individual, then the PIA will require a System of Records Notice (SORN). A SORN is a group of records (paper, electronic) from which PII is retrieved using the name of the individual or some other identifying number, symbol or particular that is unique to the individual. The SORN notifies the general public what personal data is being collected, the purpose of the collection and the authority for doing so. It also sets the rules to follow in collecting and maintaining the personal data.

5. A DCI collects, maintains, uses and/or disseminates PII about members of the public, DoD personnel (government civilians, members of the military and non-appropriated fund employees), contractors or foreign nationals employed at U.S. military facilities.

6. Army policy requires that PIAs for all DCIs be submitted using DoD DD Form 2930, which is available at the DoD Forms Management web site (<http://www.dtic.mil/whs/directives/infomgt/forms/eforms/dd2930.pdf>).

7. If the DCI collects information on 10 or more members of the public, the system and/or application owner must obtain Office of Management Budget (OMB) approval. The OMB control number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period.

8. If the DCI does not collect, maintain or disseminate PII, the DCI owner only needs to complete Sections 1, 2a, 2b, 3e and the first three signature blocks in Section 4 of DD Form 2930.

9. A PIA is not required when the DCI has been designated a National Security System (NSS), to include systems that process classified information. Subchapter III (Information Security), Chapter 35, Title 44 states that the head of each agency operating or exercising control of an NSS shall be responsible for ensuring that the agency:

a. Provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification or destruction of the information contained in such system.

b. Implements information security policies and practices, as required by standards and guidelines for NSS, issued in accordance with law and as directed by the president; and complies with the requirements of this subchapter.

SAIS-CBA

SUBJECT: Guidance for Submission of Privacy Impact Assessments (PIAs)

10. The DCI must be registered in the Army Portfolio Management Solution (APMS) or Medical Information Systems Registry (MISR). The portfolio management systems are used for two primary functions:

a. Compliance reporting, including for the Federal Information Security Management Act (FISMA), Privacy and PIAs, the Clinger-Cohen Act and Public Key Infrastructure (PKI) requirements.

b. IT investment management requirements at the enterprise, mission area, domain and command levels.

11. PIAs for Army Medical Command (MEDCOM) DCIs are processed according to their funding source. The DCIs purchased with Defense Health Program funds must follow the Army MEDCOM PIA procedures. Army MEDCOM DCIs purchased with Army funds will follow the Army CIO/G-6 PIA procedures outlined in this memorandum.

12. Tenants must identify all PII (i.e., personal, financial, medical, military) residing on Network Enterprise Centers systems and service provider systems, networks and storage area networks, and all PII embedded within applications, by completing a DO Form 2930 PIA to be submitted as part of the Tenant Security Plan.

13. The DCI for which the PIA is written must have an Authorization to Operate (ATO) or Certificate of Networkiness (CoN), or be a registered/unregistered child to a parent DCI in APMS prior to operation. If the DCI is standalone, it must have a registered DoD IT Portfolio Repository/Army Information Technology Registry (DITPRIA/TR) number.

14. PIAs must be reviewed and updated as follows:

a. When there is a significant change in data collection or in the privacy or security posture.

b. Annually in conjunction with the annual information assurance controls re-validation.

c. Within three years of PIA approval date in accordance with FISMA requirements.

15. All PIA submissions must go through the local command privacy official or PIA point of contact (POC).

16. Procedures for submitting a PIA are delineated in Department of the Army Pamphlet 25-1-1.

SAIS-CBA

SUBJECT: Guidance for Submission of Privacy Impact Assessments (PIAs)

17. All PIAs that identify information collected from members of the general public and federal personnel and/or contractors will be displayed on the Army CIO-G-6 website (<http://ciog6.army.millprivacyimpactassessments/tabid/71/default.aspx>).

18. This memorandum is effective immediately and supplements other Army CIO/G-6 PIA guidance. This updated guidance will be in effect until superseded by the next revision of AR 25-1.

19. Comments or questions concerning privacy and SORN should be directed to the Army Privacy Office: Ms. Katura Reese, katura.m.reese.civ@mail.mil, DSN 328-6193 or (703) 428-6193; Mr. Leroy Jones, DSN 328-6185, (703) 428-6185 or leroy.jones68.civ@mail.mil; or the Army Privacy Office general mailbox, usarmy.belvoir.hqda-oaa-aha.mbx.rmda-foia-privacy-alert@mail.mil.

20. Comments or questions on PIAs should be directed to CIO/G-6: Ms. Cynthia K. Dixon, DSN 865-1545, (703) 545-1545 or cynthia.k.dlxon2.civ@mail.mil; and Ms. Mary Jackson, DSN 865-1532, (703) 545-1532 or mary.c.jackson.civ@mail.mil. Inquires and completed PIAs may also be sent to the general CIO/G-6 PIA mailbox: CIO-G6.PIA.inbox@mail.mil.

Encl

1M!JJ2
MICHAEL E. KRIEGER
Acting Chief Information Officer/G-6

DISTRIBUTION:

Principal Officials of Headquarters, Department of the Army
Commander

U.S. Army Forces Command

U.S. Army Training and Doctrine Command

U.S. Army Materiel Command

U.S. Army Europe

U.S. Army Central

U.S. Army North

U.S. Army South

U.S. Army Pacific

U.S. Army Africa

U.S. Army Special Operations Command

Military Surface Deployment and Distribution Command

U.S. Army Space and Missile Defense Command/Army Forces Strategic Command

SAIS-CBA

SUBJECT: Guidance for Submission of Privacy Impact Assessments (PIAs)

U.S. Army Network Enterprise Technology Command/9¹_h Signal Command (Army)
U.S. Army Medical Command
U.S. Army Intelligence and Security Command
U.S. Army Criminal Investigation Command
U.S. Army Corps of Engineers
U.S. Army Military District of Washington
U.S. Army Test and Evaluation Command
U.S. Army Installation Management Command
Superintendent, United States Military Academy
Director, U.S. Army Acquisition Support Center

CF:

Commander, U.S. Army Cyber Command
Commander, U.S. Army Reserve Command
Director, Army National Guard
Director of Business Transformation
Executive Director, Army National Cemeteries Program

ENCLOSURE

Examples of Personally Identifiable Information (PII) and Data Collection Instruments (DCIs)

1. PII is used to distinguish or trace an individual's identity and includes information such as name, social security number, biometric records, date and place of birth, and mother's maiden name. When used alone or combined with other personal or identifying information, PII can be linked to a specific individual. As it pertains to DoD, DCIs used to collect, maintain or disseminate PII of the general public, DoD personnel (government civilians, members of the military and non-appropriated fund employees), contractors and, in some cases, foreign nationals are governed by DoD 5400.11, which contains specific guidance on personal information that is normally releasable for DoD personnel.

2. For PIA purposes, DCIs include but are not limited to:

- a. Systems
- b. Applications
- c. Processes
- d. Programs
- e. Standardized queries
- f. Spreadsheets
- g. Metering and monitoring
- h. Transmission media
- i. Websites

3. Per DoD 5400.11-R, Chapter 4, Section C4.2.2.5.1, the following items of civilian employees' personal information may normally be released without a clearly unwarranted invasion of personal privacy.

- a. Name
- b. Present and past position titles
- c. Present and past grades
- d. Present and past annual salary rates
- e. Present and past duty stations

ENCLOSURE

Examples of Personally Identifiable Information (PII) and Data Collection Instruments (DCIs)

f. Office and duty telephone numbers

g. Position Descriptions

4. Per DoD 5400.11-R, Chapter 4, Section C4.2.2.5.2, the following items of military members' personal information may normally be disclosed without a clearly unwarranted invasion of their personal privacy.

a. Name

b. Rank

c. Date of rank

d. Gross salary

e. Past duty assignments

f. Present duty assignment

g. Future assignments that are officially established

h. Office or duty telephone numbers

i. Source of commission

j. Promotion sequence number

k. Awards and decorations

l. Attendance at professional military schools

m. Duty status at any given time

n. Home of record (identification of the state only)

o. Length of military service

p. Basic pay entry date

q. Official photo

ENCLOSURE

Examples of Personally Identifiable Information (PII) and Data Collection Instruments (DCIs)

5. Per DoD 5400.11-R, Chapter 4, Section C4.2.2.5.3, the following items of information for civilian employees not under the authority of Office of Personnel Management and non-appropriated fund employees may normally be released without a clearly unwarranted invasion of personal privacy.

- a. Full name
- b. Grade or position
- c. Date of grade
- d. Gross salary
- e. Present and past assignments
- f. Future assignments, if officially established
- g. Office or duty telephone numbers