



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Electronic Military Personnel Records System (EMPRS)

Program Manager

Department of the Navy

Navy Personnel Command
Business Operations Department
IT-IM Division (Pers-34)

Mark Gill

(901) 874-3307

DSN 882-3307

INTRODUCTION

Privacy Impact Assessment (PIAs) are conducted on IT systems (including in development, purchased, operational, and significantly modified), electronic collections, and IT projects in order to:

- (1) Ensure personally identifiable information (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.

In addition to the OMB requirement of performing PIAs for PII about members of the public (Reference (b)), the Department of Defense requires that PIAs be performed when PII about Federal personnel, DoD contractors and, in some cases, foreign nationals (e.g., foreign nationals employed at U.S. military facilities internationally) is collected, maintained, used, or disseminated in electronic form.

IMPORTANT: ALL fields are required unless otherwise stated. For additional assistance see your Privacy Officer.

PIAs consist of four sections:

Section 1: Is a PIA Required?

Section 2: PIA Summary Information

Section 3: PIA Questionnaire

Section 4: Review and Approval Signatures

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a. Each DoD Component will maintain a central repository of its PIAs on the Component's public Web site until PII is no longer maintained in the system or the system is not in operation.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. If the PIA document or summary contains information that would raise security concerns, reveal classified information (i.e., national security) or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort, or competitive business interest), the DoD Component can restrict the publication of the assessment. Such information shall be protected and handled consistent with section 552 of Reference (g).

SUBMISSION:

DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at pia@osd.mil. The DoD CIO PIA Web Site will be the central link to the Component PIA Web sites.

SECTION 1: IS A PIA REQUIRED?

a. Will this IT system, electronic collection, or IT project collect, maintain, use, and/or disseminate PII about members of the public, Federal employees (personnel), DoD contractors and, in some cases, foreign nationals? Choose one option from the choices below. (Choose (3) for foreign nationals.

- (1) Yes, from members of the general public.
- (2) Yes, from Federal employees and/or Federal contractors.
- (3) Yes, from both members of the general public, Federal employees and/or Federal contractors.
- (4) No.

b. If "No," ensure the authoritative database that updates DoD IT Portfolio Repository (DITPR) is annotated for the reasons why a PIA is not required. If the IT system, electronic collection, or IT project is not in the DITPR, ensure that the reasons are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Name of IT system, electronic collection, or IT project. Electronic Military Personnel Records System (EMPRS)

b. Why is this PIA being created. Choose one:

- New IT System
- New Electronic Collection
- New IT Project
- Existing IT System
- Existing Electronic Collection
- Existing IT Project
- Significantly Modified IT System
- Significantly Modified Electronic Collection
- Significantly Modified IT Project
- Other

c. DoD Component. Choose one:

<input type="checkbox"/> AFIS	<input type="checkbox"/> DFT	<input type="checkbox"/> DTRMC	<input type="checkbox"/> USAFRICOM
<input type="checkbox"/> ARMY	<input type="checkbox"/> DHRA	<input type="checkbox"/> DRSA	<input type="checkbox"/> USCENTCOM
<input type="checkbox"/> ASD(HA)	<input type="checkbox"/> DIA	<input type="checkbox"/> GC	<input type="checkbox"/> USD(AT&L)
<input type="checkbox"/> ASD(HR)	<input type="checkbox"/> DISA	<input type="checkbox"/> IADB	<input type="checkbox"/> USD(C)
<input checked="" type="checkbox"/> ASD(ISA)	<input type="checkbox"/> DLA	<input type="checkbox"/> JOINT STAFF	<input type="checkbox"/> USD(I)
<input type="checkbox"/> ASD(ISP)	<input type="checkbox"/> DLSA	<input type="checkbox"/> MDA	<input type="checkbox"/> USD(P)
<input type="checkbox"/> ASD(LA)	<input type="checkbox"/> DMA	<input checked="" type="checkbox"/> NAVY	<input type="checkbox"/> USD(P&R)
<input type="checkbox"/> ASD(NII)	<input type="checkbox"/> DMDC	<input type="checkbox"/> NCBDP	<input type="checkbox"/> USEUCOM
<input type="checkbox"/> ASD(PA)	<input type="checkbox"/> DNA	<input type="checkbox"/> NDU	<input type="checkbox"/> USJFCOM
<input type="checkbox"/> ASD(RA)	<input type="checkbox"/> DODEA	<input type="checkbox"/> NG	<input type="checkbox"/> USMC
<input type="checkbox"/> ASD(SO/LIC)	<input type="checkbox"/> DODFP	<input type="checkbox"/> NORAD	<input type="checkbox"/> USNATO
<input type="checkbox"/> BTA	<input type="checkbox"/> DODIF	<input type="checkbox"/> NRO	<input type="checkbox"/> USNORTHCOM
<input type="checkbox"/> CIFA	<input type="checkbox"/> DOT&E	<input type="checkbox"/> OEA	<input type="checkbox"/> USPACOM
<input type="checkbox"/> DA&M	<input type="checkbox"/> DPA&E	<input type="checkbox"/> OSD(CIO)	<input type="checkbox"/> USSOCOM
<input type="checkbox"/> DARPA	<input type="checkbox"/> DPMO	<input type="checkbox"/> PFPA	<input type="checkbox"/> USSOUTHCOM
<input type="checkbox"/> DCAA	<input type="checkbox"/> DSCA	<input type="checkbox"/> SECDEF	<input type="checkbox"/> USSTRATCOM
<input type="checkbox"/> DCMA	<input type="checkbox"/> DSS	<input type="checkbox"/> SECNAV	<input type="checkbox"/> USTRANSCOM
<input type="checkbox"/> DECA	<input type="checkbox"/> DTIC	<input type="checkbox"/> TMA	<input type="checkbox"/> WHS
<input type="checkbox"/> DFAS	<input type="checkbox"/> DTRA	<input type="checkbox"/> USAF	<input type="checkbox"/> OTHER

d. DITPR System Identification Number(s), as applicable. 0109

e. Budget System Identification Number (Select and Native Programming Data Input System – Information Technology (SNAP-IT) Initiative Number), as applicable.

0737

f. IT Investment Unique Project Identifier, as required by section 53 of OMB Circular A-11, as applicable. 007-17-01-20-01-0737-00-201-067

g. Does the IT system, electronic collection, or IT project require a Privacy Act SORN Identifier?

Yes

No

(1) If "Yes," enter the Privacy Act SORN Identifier (this is the DoD Component-assigned designator and not the Federal Register number). N01070-3

(2) If the Privacy Act SORN is not yet published, when will it be published?

Enter date or "unknown": N/A

h. OMB Control Number, as applicable. N/A

i. OMB Control Number expiration date, as applicable. N/A

j. Authority to collect information. A Federal law, Executive Order of the President (EO), or requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same. If new authorities are identified in this PIA, the Privacy Act SORN must be altered.

(2) Describe the authority for this IT system, electronic collection, or IT project to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, describe each.)

(a) Whenever possible cite the specific provisions of the statute and/or Executive Order (EO) that authorizes the operation of the system and the collection of PII.

(b) If a specific statute and/or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority statute ("internal housekeeping") as the primary authority. The requirement, directive or instruction implementing the statute within the DoD Component should be identified.

The information contained within EMPRS is protected by the Privacy Act of 1974, which provides for limiting the disclosure of personal information; requires accurate, timely, relevant, and complete records; and requires safeguards that ensure the confidentiality and security of records.

10 U.S.C. 5013, Secretary of the Navy; 42 U.S.C. 10606 as implemented by DoD Instruction 1030.1, Victim and Witness Assistance Procedures; and E.O. 9397 (SSN).

BUPERS Instruction 5239.1B, Bureau of Naval Personnel (BUPERS) Information Systems Security (INFOSEC) Program, April 5, 2001

CJCSI 6510.01, Chairman of the Joint Chiefs of Staff Instruction, Defense in Depth: Information Assurance (IA) and Computer Network Defense (CND), March 18, 2005

DoDI 8510.01, Department of Defense, Information Assurance Certification and Accreditation Process (DIACAP) Instruction, 28 NOV 2007

DoN IA Publication 5239-13 Volume I, Introduction to Certification and Accreditation, December 2000

DoN IA Publication 5239-13 Volume II, Site, Installed Program of Record, and Locally Acquired Systems, December 2000

DoN IA Publication 5239-13 Volume III, Program of Record/Deployable Information Systems, October 2003

BUPERSINST 5211.6, Bureau of Naval Personnel Instruction, Compliance with the Privacy Act and Protection of Personally Identifiable Information (PII), 14 April 2008

k. How will the information be collected? (Indicate all that apply.)

- Paper Form Face-to-Face Contact Telephone Interview Fax
 E-mail Web site Information Sharing from System to System
 Other

If "Other", provide explanation:

l. Summary of IT system, electronic collection, or IT project.

(1) What is the purpose and general activity of this IT system, electronic collection, or IT project?

EMPRS maintains the single authoritative, official personnel record images for Navy military members. Documents are received either via regular mail or electronically for input into the system. These digital images are provided to authorized users to support Casualty Management, Mobilization, Career Management, Distribution, and other personnel and manpower management functions. EMPRS will allow on-line, authenticated access capability via the BUPERS OnLine (BOL) IT system.

(2) For new IT systems (including in development or purchased) describe the reasons for the final IT design choice or business process.

N/A