



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a. Each DoD Component will maintain a central repository of its PIAs on the Component's public Web site until PII is no longer maintained in the system or the system is not in operation.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

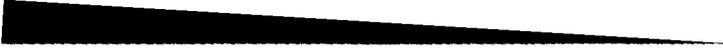
0737

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). NO1070-3

(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



SECTION 3: PIA QUESTIONNAIRE

a. For the questions in subparagraphs 4.a.(1) through 4.a.(4), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all that apply.

<input checked="" type="checkbox"/> Name	<input checked="" type="checkbox"/> Other Names Used	<input checked="" type="checkbox"/> Social Security Number (SSN)
<input checked="" type="checkbox"/> Truncated SSN	<input checked="" type="checkbox"/> Drivers License	<input type="checkbox"/> Other ID Number
<input checked="" type="checkbox"/> Citizenship	<input checked="" type="checkbox"/> Legal Status	<input checked="" type="checkbox"/> Gender
<input checked="" type="checkbox"/> Race/Ethnicity	<input checked="" type="checkbox"/> Birth Date	<input checked="" type="checkbox"/> Place of Birth
<input type="checkbox"/> Personal Cell Telephone	<input checked="" type="checkbox"/> Home Telephone Numbers	<input checked="" type="checkbox"/> Personal Email Address
<input checked="" type="checkbox"/> Mailing/Home Address	<input checked="" type="checkbox"/> Religious Preference	<input checked="" type="checkbox"/> Security Clearance
<input checked="" type="checkbox"/> Mother's Maiden Name	<input checked="" type="checkbox"/> Mother's Middle Name	<input checked="" type="checkbox"/> Spouse Information
<input checked="" type="checkbox"/> Marital Status	<input checked="" type="checkbox"/> Biometrics	<input checked="" type="checkbox"/> Child Information
<input type="checkbox"/> Vehicle Identifiers	<input checked="" type="checkbox"/> Medical Information	<input checked="" type="checkbox"/> Disability Information
<input type="checkbox"/> Financial Information	<input checked="" type="checkbox"/> Employment Information	<input checked="" type="checkbox"/> Military Records
<input checked="" type="checkbox"/> Law Enforcement Information	<input checked="" type="checkbox"/> Emergency Contact	<input checked="" type="checkbox"/> Education Information
<input checked="" type="checkbox"/> Military Rank*	<input type="checkbox"/> Civilian Grade*	<input type="checkbox"/> Other, Specify

* Military Rank and Civilian Grade are typically treated as "For Official Use Only." As such, release of either to a member of the public must be coordinated through Component Freedom of Information Office.

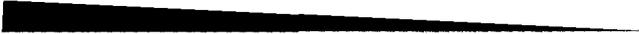
If "Other", specify:

(2) What is the nature or source for each PII collected (e.g., individual, existing DoD IT system, other Federal database, commercial systems)?

Describe: Individuals/service members and existing Navy IT Corporate Systems (Naval Personnel Evaluation System (NPES), Naval Personnel Database (NPDB), Navy Enlisted Personnel System (NES), Officer Personnel Information System (OPINS), Inactive Manpower and Personnel Management Information System (IMAPMIS)

(3) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

Describe: Verification, identification, authentication and data matching to enable record management capabilities associated with building the Official Military Personnel File (OMPF). EMPRS is a primary input point for forms and data utilized to build the OMPF and to facilitate the promotion/selection process for career progression.



(4) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

Describe: To assist officials and employees of the Navy in the management, supervision and administration of Navy personnel (officer and enlisted) and the operations of related personnel affairs and functions. EMPRS PII is a crucial element in the development and maintenance of the OMPF and is especially vital during all aspects of the promotion/selection process. Additionally, other government and law enforcement agencies use this data to validate employment history, security background information, next of kin, etc. Active and former service members can request copies of OMPF records via paper and electronic media (Encrypted CD-ROM).

b. With whom will the PII be shared, both within the DoD Component and outside the Component (e.g., other DoD Components, Federal agencies)? Indicate all that apply.

- Within the DoD Component. Specify: Individuals/service members, Command representatives, NCIS and Selection Boards
- Other DoD Components. Specify: DCIS, IG, Defense Personnel Record Information System (DPRIS)
- Other Federal Agencies. Specify: VA, DHS, DOL, FBI, CIA and other law enforcement agencies
- State and Local Agencies. Specify: Law enforcement agencies
- Contractor. Specify (State contractor's name and describe the language in the contract that safeguards PII.):
- Other (e.g., commercial provider, colleges). Specify:

c. Do individuals have the opportunity to object to the collection of PII about themselves?

- Yes
- No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

Secretary of the Navy (SECNAV) Instruction 5211.5; 32 CFR part 701

(2) If "No," state the reason why individuals cannot object.

d. Do individuals have the opportunity to consent to the specific uses of their PII?

- Yes
- No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

Secretary of the Navy (SECNAV) Instruction 5211.5; 32 CFR part 701

(2) If "No," state the reason why individuals cannot give or withhold their consent.

e. Does system create or derive new PII about individuals through data aggregation?

Yes

No

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

f. What information is provided to an individual? (Indicate all that apply.)

Privacy Act Statement Privacy Advisory Other None

Describe each applicable format.

Required FOUO and Privacy Act disclaimers are displayed throughout the site. The DoD required Privacy and Monitoring Advisory is available on login.

g. Who will have or has access to PII on the system? (Indicate all that apply.)

Users Developers System Administrators Contractors

Other, specify:

h. How will the PII be secured?

(1) Physical Controls. (Indicate all that apply)

Security Guards, Cipher Locks Identification Badges
 Biometrics Key Cards Closed Circuit Television
 Common Access Cards Other, describe:

(2) Technical Controls. (Indicate all that apply)

User Identification Biometrics Intrusion Detection System
 Firewall Password Virtual Private Network
 Encryption DoD Public Key Infrastructure Certificates



External Certificate Authority Certificate

Other, describe:

(3) Administrative Controls. (Indicate all that apply)

Perform Periodic Security Audits

Frequency: Monthly

Regular Monitoring of Users' Security Practices

Limited Access of Users to Equipment and Information

Encryption of Backups When They Contain Sensitive Data

Keep Extra Backups Off-Site in a Locked Fireproof Location

Methods in Place to Ensure Only Authorized Personnel Have Access to PII

Other, describe:

(4) Additional Controls. Describe any additional controls not listed above, or comment on any of the responses above indicating how PII will be secured.

The National, DoD, and Service security requirements are derived from the following National, Department of Defense (DoD), and Service specific directives and instructions and are applicable to EMPRS.

- a. Executive Order 12958
- b. Public Law 100-235
- c. OMB Circular A-130
- d. DoDD 8500.1
- e. DoDI 8500.
- f. OPNAVINST 5239.1B
- g. SECNAVINST 5239.3A
- h. SECNAV Instruction 5510.30A
- i. SECNAV Instruction 5510.36
- j. BUPERS Instruction 5239.1B
- k. Navy-Marine Corps Unclassified Trusted Network Protection (UTNProtect) Policy

Customary Personnel and Technical Security Controls mandated for all Department of the Navy systems (i.e., Identification and Authentication, Audit, File Access Control, etc.) have been incorporated at the operating system level and evaluated in the EMPRS System Security Authorization Agreement (SSAA).



i. Has your IT system undergone a certification and accreditation process?

Yes

No

Not Required

(1) If "Yes," what is the current status?

Authorization to Operate

Interim Authorization to Operate

Interim Authorization to Test

Denial of Authorization to Operate

None-Not Yet Accredited

(2) On what date was the current certification and accreditation status granted? 09 Jul 2008

j. Considering the "information life cycle" (i.e., collection, use, retention, processing, disclosure, and destruction), evaluate and describe how information handling practices at each stage may affect individuals' privacy.

PII data from individuals and external corporate IT systems enables verification, authentication identification and data matching necessary for records management and access control. Official information received for inclusion in the EMPRS record is scanned (digitized) into the core record and the original paper documents are shredded. Once in the system, access is limited to individuals and agencies with documented need-to-know and user/password authentication. Digitized documents will be retained per Federal law for 80 years (minimum). For the Selection Board Process (a closed/isolated, internal system with highly restricted access), PII data is captured from corporate mainframe system through a secure server-to-server connection, via the TECTIA Secure File Transfer Protocol. Upon validated request, authorized personnel will be provided copies of individual records via an encrypted CD-Rom coupled with password security method.

k. Identify the privacy risks to the individual associated with data collection and data flow.

a) Intrusion into EMPRS by unauthorized personnel; mitigated through the use of PKI, Firewall, restricted access to files based on user permissions.

b) Copy of OMPF CD-ROM falling into unauthorized person's possession; mitigated through the use of a AES 128 bit encryption of the CD-ROM files, coupled with password activation method.



i. Describe the appropriate measures to mitigate the identified privacy risks.

Mitigation discussed in previous paragraph K.

