



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Employee Master Maintenance Application (EMMA)

Department of the Navy - NAVAIR

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

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

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

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

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

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- New DoD Information System New Electronic Collection
- Existing DoD Information System Existing Electronic Collection
- Significantly Modified DoD Information System

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR Enter DITPR System Identification Number

DITPR ID: 8131 DITPR DON ID: 21605

- Yes, SIPRNET Enter SIPRNET Identification Number

--
- No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes No

If "Yes," enter UPI

UII: 007-000001961

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- Yes No

If "Yes," enter Privacy Act SORN Identifier

NM01500-2; NM05000-2; NM07421-1

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office

Consult the Component Privacy Office for this date.

--

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

Yes

Enter OMB Control Number

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD 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.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

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

(b) If a specific statute 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 ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

SORN authorities:

NM01500-2

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps function, composition
OPNAVINST 1510.10B, Corporate Enterprise Training Activity Resource System (CeTARS), Catalog of Navy Training Courses and Student Reporting Requirements
MCO 1580.7D Schools Inter-service Training
E.O. 9397 (SSN), as amended.

NM05000-2

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
E.O. 9397 (SSN), as amended.

NM07421-1

5 U.S.C. 301, Departmental Regulations

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
E.O. 9397 (SSN), as amended.

Other authorities:

FRCSEINST3500.2 TRAINING AND EMPLOYEE DEVELOPMENT

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

This program maintains a current personnel listing and tracks and maintains training records for all personnel in order to report required training.

DTS Packages are built to extract Personal, Shop, and QA Data to be replicated in the Internal Defect Reporting System (IDRS) and to the Quality Workbench (QAWB).

DCPDS Export used to populate Excel Spreadsheets to update DCPDS records. Spreadsheets are encrypted.

PII Collected: Full Name, SSN, On Board Date, Hire Date, Position information:: job description, Payroll ID#, employment information: work history; education information: level of education completed, name of school (s), Degree, classes taken, and training and certifications.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Identity theft: This system is locked down by permissions only and no one has access to PII except for a few high level personnel with a need to know. Upon entry of the system a banner identifies a Privacy Act Statement notifying individuals that the system contains PII information and their responsibility to maintain.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

Within the DoD Component.

Specify.

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

- Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

NTA, Tyonek, Sobran, GDIT

Work under this task order requires access to personally identifiable information (PII) and information protected by the Privacy Act of 1974. In addition to the security requirements below, contractors performing work under this task order must meet the following criteria: Per SECNAV M-5510.30, all individuals with access to PII or Privacy Act information must be US Citizens; therefore US Citizenship is a requirement. In all cases contract employees must meet eligibility requirements for a position of trust at a minimum. The contractor shall comply with all applicable DoD security regulations and procedures during the performance of this task order. Contractor shall not disclose and must safeguard procurement sensitive information, computer systems and data, privacy act data, sensitive but unclassified (SBU) information, classified information, and all government personnel work products that are obtained or generated in the performance of this task order. Contractor employees are required to have National Agency Check, Local Agency Check and Local Credit Check (NACLC) investigation at a minimum in accordance with DoD Instruction 8500.2. Local Agency Check and Local Credit Check must be submitted and results received prior to commencement of work. A security clearance may also be required to perform work under this contract.

- Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

- Yes** **No**

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

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

The PII must be collected to ensure that the artisans are qualified to work on platform specific equipment and functions. Condition of employment.

j. 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.

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

The PII must be collected to ensure that the artisans are qualified to work on platform specific equipment and functions. Condition of employment.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- | | |
|--|--|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

Information is provided to individuals in paper form at time of employment.

Authority: 5 U.S.C 4103 and 4118

Purpose: The purpose of this system is to maintain a listing of training, education, and qualifications of Department of the Navy personnel for use by Manpower, Personnel and Training managers. This system will also be used to provide projections of training resources.

Routine Use (s): The information will be used by employees, officials and/or contractors of the DON in the performance of their official duties relating to their management of the Command's civilian/military employee training programs, record keeping screening and selection of candidates centrally - administered programs; and the administration of grievance appeals, complaints, and litigation involving the disclosure of records of the training program.

Disclosure: Voluntary; failure to provide the information may result in the training not being posted to the individual's training record.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

- Name Other Names Used Social Security Number (SSN)
- Truncated SSN Driver's License Other ID Number
- Citizenship Legal Status Gender
- Race/Ethnicity Birth Date Place of Birth
- Personal Cell Telephone Number Home Telephone Number Personal Email Address
- Mailing/Home Address Religious Preference Security Clearance
- Mother's Maiden Name Mother's Middle Name Spouse Information
- Marital Status Biometrics Child Information
- Financial Information Medical Information Disability Information
- Law Enforcement Information Employment Information Military Records
- Emergency Contact Education Information Other

If "Other," specify or explain any PII grouping selected.

Other ID Number: Payroll ID #;
 Other: On Board Date, Hire date, Position Information: job description;
 Employment information: work history;
 Education information: level of education completed, name of school(s), Degree, classes taken, and training and certifications.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

PII is provided by the individual upon employment and entered into EMMA by system administrators in order to track training and job specific qualifications.

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

- | | |
|---|--|
| <input checked="" type="checkbox"/> Paper Form | <input checked="" type="checkbox"/> Face-to-Face Contact |
| <input checked="" type="checkbox"/> Telephone Interview | <input type="checkbox"/> Fax |
| <input type="checkbox"/> Email | <input type="checkbox"/> Web Site |
| <input type="checkbox"/> Information Sharing - System to System | |
| <input type="checkbox"/> Other | |

If "Other," describe here.

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

Verification: Records are being collected and maintained for admin-related purposes of tracking and verifying individual completion of required training and training that is required for specific jobs.

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

Mission-related and Administrative Use: To ensure employees have taken required training for their position to enable employee to complete the mission assigned.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

Yes No

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

c. Who has or will have access to PII in this DoD information system or electronic collection? Indicate all that apply.

- Users Developers System Administrators Contractors
 Other

EEO, Legal, Personnel Security Manager, Information Assurance Manager, Quality Assurance, Safety, Travel employees and a few Senior level management secretaries. Additionally, contractor employees who work for training and contractor managers for their employees will have visibility of PII. For the purpose of verifying training accomplished and identifying individuals in case of an emergency.

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

- Security Guards Cipher Locks
 Identification Badges Combination Locks
 Key Cards Closed Circuit TV (CCTV)
 Safes Other

Servers are protected in a dual point authenticated computer room. Computer room access list are reviewed every 90 days. Visitors to computer room sign log book per DODI 8500.2 access controls.

(2) Technical Controls. Indicate all that apply.

- User Identification Biometrics
 Password Firewall
 Intrusion Detection System (IDS) Virtual Private Network (VPN)
 Encryption DoD Public Key Infrastructure Certificates
 External Certificate Authority (CA) Certificate Common Access Card (CAC)
 Other

Discretionary access control.

(3) Administrative Controls. Indicate all that apply.

- Periodic Security Audits**
- Regular Monitoring of Users' Security Practices**
- Methods to Ensure Only Authorized Personnel Access to PII**
- Encryption of Backups Containing Sensitive Data**
- Backups Secured Off-site**
- Other**

Administrative access controls are validated against required DODI 8500.2 controls.

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

- Yes. Indicate the certification and accreditation status:**

- | | | | |
|-------------------------------------|--|----------------------|---------------------------------------|
| <input checked="" type="checkbox"/> | Authorization to Operate (ATO) | Date Granted: | <input type="text" value="20140703"/> |
| <input type="checkbox"/> | Interim Authorization to Operate (IATO) | Date Granted: | <input type="text"/> |
| <input type="checkbox"/> | Denial of Authorization to Operate (DATO) | Date Granted: | <input type="text"/> |
| <input type="checkbox"/> | Interim Authorization to Test (IATT) | Date Granted: | <input type="text"/> |

- No, this DoD information system does not require certification and accreditation.**

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Collection, Use, Processing: The employee file is created from employee information entered from TAA or manually. Training is entered at the time of completion against the PII information. Administrative staff completes training information daily. Training data is pulled and provided for data calls upon request.

Disclosure: Direct managers may see Training accomplished for their employees. Database administrators and a select few of individuals who have a need to know are permitted to see all records. The System displays a PII banner upon entering the program.

Retention/Destruction: Training accomplished data is maintained for the life of the employee's employment. Upon the employee's departure from the command the data is transferred to inactive and archived. Retention of this data shall be in accordance with SECNAV M5210-1, Records Management Manual (SSIC 5230.2 applies)

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

The perceived threats are primarily computer hackers, disgruntled employees, state sponsored information warfare, and acts of nature (e.g., fire, flood, etc.).

All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that EMMA, with its extensive collection of PII, could be compromised.

Because of this possibility, appropriate security and access controls listed in this PIA are in place.

Since EMMA operates on the local Fleet Readiness Center network, there is a risk that security controls could be disabled for maintenance and other purposes. The risk would be that the security controls would not be reset.

All systems are vulnerable to "insider threats". EMMA managers are vigilant to this threat by limiting system access to those individuals who have a defined need to access the information. There are defined criteria to identify who should have access to EMMA data. These individuals have gone through extensive background and employment investigations.

Mitigations:

The following controls are used to mitigate the risks:

- a) Access Controls.
Access to individual computers are controlled by Common Access Card (CAC) or user-id and password protected. Access to the application is verified by their NMCI Logon and permissions in the program.
- b) Confidentiality.
Specific users have individual permissions based on their NMCI logon and have specific roles granted within EMMA.
- c) Integrity.
There are transaction records for any changes to EMMA data.
- d) Audits.
As a training system, EMMA is reviewed during various audits throughout the year.
- e) Training.
Annual privacy awareness training is required by all employees.
- f) Physical Security.
Computer processing facilities are located in restricted areas accessible only to authorized persons that are properly screened, cleared, and trained. Manual records and computer printouts are only available to authorized personnel having a need-to-know. Building access requires badge access. Computer room access requires key or badge for access and is video monitored.

EMMA servers are currently located at FRCSE Data Center (moving to NAVAIR Patuxent River, MD by end of 2014)

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

N/A

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

**Program Manager or
Designee Signature**

SEIBERLING.LORRINDA.DEE.114182
5603 Digitally signed by SEIBERLING.LORRINDA.DEE.1141825603
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN,
cn=SEIBERLING.LORRINDA.DEE.1141825603
Date: 2013.09.05 12:41:27 -04'00'

Name: Lorrinda Seiberling

Title: Career Development Division Director (code 73300)

Organization: FRCSE

Work Telephone Number: 904 790-5690

DSN: 690-5690

Email Address: lorrinda.seiberling@navy.mil

Date of Review: 05Sep2013

**Other Official Signature
(to be used at Component
discretion)**

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

**Other Official Signature
(to be used at Component
discretion)**

WEISS.MITCHEL.122874
8672 Digitally signed by WEISS.MITCHEL.1228748672
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=USN, cn=WEISS.MITCHEL.1228748672
Date: 2014.08.05 14:02:14 -04'00'

Name: Mitchel Weiss
Title: Privacy Act Officer
Organization: FRCSE
Work Telephone Number: 904-790-5408
DSN:
Email Address: mitchel.weiss@navy.mil
Date of Review: 20140805

**Component Senior
Information Assurance
Officer Signature or
Designee**

GADDIST.KEVIN
.K.1022467340 Digitally signed by
GADDIST.KEVIN.K.1022467340
DN: c=US, o=U.S. Government, ou=DoD,
ou=PKI, ou=USN,
cn=GADDIST.KEVIN.K.1022467340
Date: 2014.08.06 06:32:05 -04'00'

Name: Kevin Gaddist
Title: IAM
Organization: Fleet Readiness Center Southeast
Work Telephone Number: 9047904513
DSN: 6904513
Email Address: kevin.gaddist@navy.mil
Date of Review: 20140806

**Component Privacy Officer
Signature**

PATTERSON.ROBIN.W.1229
323403 Digitally signed by PATTERSON.ROBIN.W.1229323403
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=USN, cn=PATTERSON.ROBIN.W.1229323403
Date: 2014.09.09 18:41:22 -04'00'

Name: Robin Patterson
Title: Head, FOIA/Privacy Act Program Office (OPNAV DNS-36)
Organization: Office of the Chief of Naval Operations (CNO)
Work Telephone Number: 202-685-6545
DSN:
Email Address: robin.patterson@navy.mil
Date of Review:

**Component CIO Signature
(Reviewing Official)**

MUCK.STEVEN.ROBERT.117
9488597
Digitally signed by MUCK.STEVEN.ROBERT.1179488597
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=USN, cn=MUCK.STEVEN.ROBERT.1179488597
Date: 2014.09.10 12:57:12 -04'00'

Name:	For Barbara Hoffman
Title:	Principal Deputy CIO
Organization:	Office of the Department of the Navy Chief Information Officer (DON CIO)
Work Telephone Number:	703-695-1842
DSN:	
Email Address:	barbara.hoffman@navy.mil
Date of Review:	10 September 2014

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/ comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.