



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Corporate Data Warehouse (CDW)

Department of the Navy - NAVSEA

### **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: 22837    DITPR DON ID: 17447
- 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: 007-000004010

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 NM05000-2, DPR 34 DoD, N07220-1, N01080-1, T7335

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.

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.

N07220-1:

10 U.S.C. 5013, Secretary of the Navy;  
E.O. 9397 (SSN), as amended.

N01080-1:

10 U.S.C. 5013, Secretary of the Navy;  
Department of Defense Instructions DoDI 1336.08, Military Human Resource Records Life Cycle Management;  
DoDI 1336.05, Automated Extract of Active Duty Military Personnel Records;  
DoDI 7730.54, Reserve Components Common Personnel Data System (RCCPDS);  
Chief of Naval Operations Instructions OPNAVINST 1070.2 Series, Automated Extracts of Active Duty Military Personnel Records;  
OPNAVINST 1001.19 Series, Reserve Components Common Personnel Data System (RCCPDS);  
E.O. 9397 (SSN), as amended.

DPR 34 DoD:

5 U.S.C. 301, Department Regulations;  
5 U.S.C. Chapter 11, Office of Personnel Management;  
5 U.S.C. Chapter 13, Special Authority;  
5 U.S.C. Chapter 29, Commissions, Oaths, Records, and Reports;  
5 U.S.C. Chapter 31, Authority for Employment; 5 U.S.C. Chapter 33, Examination, Selection, and Placement;  
5 U.S.C. Chapter 41, Training; 5 U.S.C. Chapter 43, Performance Appraisal;  
5 U.S.C. Chapter 51, Classification;  
5 U.S.C. Chapter 53, Pay Rates and Systems;  
5 U.S.C. Chapter 55, Pay Administration;  
5 U.S.C. Chapter 61, Hours of Work;  
5 U.S.C. Chapter 63, Leave;  
5 U.S.C. Chapter 72, Antidiscrimination; Right to Petition Congress;  
5 U.S.C. Chapter 75, Adverse Actions;  
5 U.S.C. Chapter 83, Retirement;  
5 U.S.C. Chapter 99, Department of Defense National Security Personnel System;  
5 U.S.C. 7201, Antidiscrimination Policy; minority recruitment program;  
10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness;  
E. O. 9830, Amending the Civil Service Rules and Providing for Federal Personnel Administration, as amended;  
29 CFR part 1614.601, EEO Group Statistics;  
E. O. 9397 (SSN), as amended.

T7335:

5 U.S.C. 301, Departmental Regulations;  
5 U.S.C. Chapter 53, 55, and 81;  
E.O. 9397 (SSN).

**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.

The NAVSEA Corporate Data Warehouse was created to house and report on information used by, but not limited to NAVSEA Headquarters. The ERP Standard Extract Files that are required for this initiative are to support the General Fund and Working Capital Fund Activities with their financial reporting and analysis needs. The data contained within these files is of a financial nature and will be utilized by financial analysts. These files are transmitted via Secure File Transfer Protocol (SFTP) from Navy ERP to an NSLC defined SFTP solution and from there into the Business Objects Environment for loading into the Oracle database. From here it is accessed by defined users, primarily within the Warfare Centers and NAVSEA Headquarters, with specific roles and need to know via the Business Objects toolset. T

The NAVSEA Corporate Data Warehouse also receives manually loaded data from NAVSEA 10 via an interface with the Defense Civilian Personnel Management Service. The NAVSEA 10 team downloads defined files from a service called HRLink. Superficially designated NAVSEA 10 team members then utilize SQL Loader scripting to load those files into the NAVSEA CDW database. From here it will be accessed by authorized NAVSEA 10 HR users, primarily within the Warfare Centers and NAVSEA Headquarters, with specific roles and need to know via the Business Objects toolset.

The PII data that comes from Navy ERP and the Defense Civilian Personnel Management Service consists of: Name, SSN, DCPDS Employee ID and DoD ID number, Citizenship, Race/Ethnicity, Birth Date, Mailing/Home Address, Security Clearance, Financial Information (Financial information would be limited to employee pay and incentive information. The annual salary and locality pay is included as well as any awards or incentives that are processed for an employee), Disability Information (Employee reported disability information is stored. Access to this information is strictly controlled to a very limited number of users, usually those in the Equal Employment Opportunity Office and developers.), Employment Information (While assigned to NAVSEA, an employee's employment record is maintained. This information includes

details and attributes concerning the position occupied or previously occupied while assigned to NAVSEA. This type of information includes data such as the Unit Identification Code, Position Description Number, Billet Identification Code, Organizational Code, Position Title, etc. Additionally data associated with an individual's qualifications necessary to occupy the position is maintained, such as the educational information, current grade, etc.), and Education Information (Employee reported Education information is stored. This information is limited to the level of education, the major field of study, year obtained and the name of the educational institution that bestowed the credentials.)

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

The system is subject to a range of generic threats similar to those applicable to most government information systems. Potential threats are natural, inherent in the system design, attributed to unauthorized personnel, and from authorized personnel who make mistakes. The system is a password controlled system as well as CAC enabled to prevent unauthorized personnel. Access to information restricted to employees with direct functional need to know. Password complexity requirements are enforced and historical logs of access are maintained and will assist in assuring only appropriate personnel have access to the database. User roles are also in place to prevent mistakes handling the data.

NAVSEA CDW utilizes the SAAR process for user registration. All database structures that contain PII are only access by properly authorized users with specific database roles assigned. Data is protected at the Business Objects report level by only allowing authorized users to the folders that contain reports with PII in them. Data is always transferred via encrypted ports (e.g. port 443 for web access).

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. NAVSEA employees - NAVSEA 10 and NAVSEA 05 Human Resource Personnel.

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. The prime company contractors are from is RGS Associates. Language in contracts - "Most of the work under this contract shall be UNCLASSIFIED. Much of the work will be Business Sensitive and/or Privacy Act protected, so the Contractor shall ensure all their personnel assigned to performance of this Task Order understand such information shall be kept "close-hold" and not disclosed outside of the respective Office, Directorate or Program Office. In addition, all ADP positions required for database support shall conform to DoD 5200.2-R requirements (especially those currently defined in Appendix C and Appendix K, Change 3, dated February 23, 1996) which identify National Agency Check guidance

and ADP Position Categories. Because of the sensitivity of information SEA 00X and SEA 10 deal with, and because of the location of the work, the following personnel requirements apply: 1. All Contractor personnel assigned to performance of this Task Order shall be U.S. citizens. 2. All contractor personnel that require access to NAVSEA sensitive or PII data shall have a SECRET clearance within 90 days of the start date of their assignment."

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.

PII is not collected directly from the individual.

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.

PII is not collected directly from the individual.

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

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

Describe each applicable format.

PII is not collected directly from the individual.

**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.

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

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

Other IDs - DCPDS Employee ID and Employee DoD ID Number.

Financial Information: Financial information would be limited to employee pay and incentive information. The annual salary and locality pay is included as well as any awards or incentives that are processed for an employee.

Disability Information: Employee reported disability information is stored. Access to this information is strictly controlled to a very limited number of users, usually those in the Equal Employment Opportunity Office and developers.

Employment Information: While assigned to NAVSEA, an employee's employment record is maintained. This information includes details and attributes concerning the position occupied or previously occupied while assigned to NAVSEA. This type of information includes data such as the Unit Identification Code, Position Description Number, Billet Identification Code, Organizational Code, Position Title, etc. Additionally data associated with an individual's qualifications necessary to occupy the position is maintained, such as the educational information, current grade, etc.

Military Information: If person is military - yes on no if they have a spouse.  
If person was military - we have dates of service, veteran status; if they are on the recall

list; if they are in reserves, years of service, and qualifications.

Education Information: Employee reported Education information is stored. This information is limited to the level of education, the major field of study, year obtained and the name of the educational institution that bestowed the credentials.

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

Existing DoD Information System:

Department of Defense Information Systems (Navy ERP and the Defense Civilian Personnel Management Service)

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

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

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

Data matching and reporting

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

Mission related use

[Empty rectangular box]

**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.

[Empty rectangular box for explanation]

**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

If "Other," specify here.

[Empty rectangular box for "Other" specification]

**d. How will the PII be secured?**

**(1) Physical controls.** Indicate all that apply.

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> Security Guards       | <input type="checkbox"/> Cipher Locks             |
| <input checked="" type="checkbox"/> Identification Badges | <input type="checkbox"/> Combination Locks        |
| <input type="checkbox"/> Key Cards                        | <input type="checkbox"/> Closed Circuit TV (CCTV) |
| <input type="checkbox"/> Safes                            | <input checked="" type="checkbox"/> Other         |

Site-specific controls are used.

The servers reside at the Defense Information Systems Agency (DISA) Mechanicsburg which is on a Navy base that only Department of Defense employees can get on to. Then you have to have access to the DISA building and those types of people either have to work there or be folks from other organizations with systems there who have a need to access the physical server. You have to have a valid security clearance and CAC. There is security guards in the building who validate who you are and grant you access to the building and the location where your systems are. The servers themselves are also in a secure area. DISA is a Navy sanctioned hosting facility

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

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> <b>User Identification</b>                  | <input type="checkbox"/> <b>Biometrics</b>  |
| <input checked="" type="checkbox"/> <b>Password</b>                             | <input type="checkbox"/> <b>Firewall</b>  |
| <input type="checkbox"/> <b>Intrusion Detection System (IDS)</b>                | <input checked="" type="checkbox"/> <b>Virtual Private Network (VPN)</b>              |
| <input checked="" type="checkbox"/> <b>Encryption</b>                           | <input checked="" type="checkbox"/> <b>DoD Public Key Infrastructure Certificates</b> |
| <input type="checkbox"/> <b>External Certificate Authority (CA) Certificate</b> | <input checked="" type="checkbox"/> <b>Common Access Card (CAC)</b>                   |
| <input type="checkbox"/> <b>Other</b>   |   |

If "Other," specify here.

**(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**

If "Other," specify here.

**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"/> <b>Authorization to Operate (ATO)</b> | <b>Date Granted:</b> | 20141210 |
| <input type="checkbox"/> <b>Interim Authorization to Operate (IATO)</b>   | <b>Date Granted:</b> |          |
| <input type="checkbox"/> <b>Denial of Authorization to Operate (DATO)</b> | <b>Date Granted:</b> |          |
| <input type="checkbox"/> <b>Interim Authorization to Test (IATT)</b>      | <b>Date Granted:</b> |          |

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: PII data from Navy ERP and NAVSEA 10 is sent via SFTP using encrypted connections. The data is loaded into Oracle Database tables via automated data processing with Business Objects. Access to these tables is limited to only those approved with an official need to know. Other PII data from NAVSEA 10 is loaded into Oracle Database tables via automated data processing with Oracle tools. Specific NAVSEA HR government staff have files located on encrypted locations on their hard drives and once they create an encrypted connection (VPN Tunnel) they can use Oracle loading tools to get the data from those files into the database tables.  
Use, Retention, and Processing: Only personnel with the "need to know" can access a member's PII information.  
Disclosure: No other personnel other than those with a "need to know" can access a member's PII information.  
Destruction: Data is destroyed in accordance with the Navy's Records Management Manual.

**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 NAVSEA CDW, 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 NAVSEA CDW is hosted by DISA and is accessible via DoD Networks, 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". Network and User 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 NAVSEA CDW. These individuals have gone through extensive background and employment investigations.

**Mitigation:**

The following controls are used to mitigate the risks:

- a) Access Controls. Access controls limit access to the application and/or specific functional areas of the application. These controls consist of privileges, password control, CAC/PKI control and discretionary access control. Additionally, each user is associated with one or more database roles. Each role provides some combination of privileges to a subset of the application tables. Users are granted only those privileges that are necessary for their job requirements. The same roles that protect the database tables also determine which buttons and menu items are enabled for the user currently logged on.
- b) Confidentiality. This ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes.
- c) Integrity. This ensures that data has not been altered or destroyed in an unauthorized manner.
- d) Audits. This includes review and examination of records, activities, and system parameters, to assess the adequacy of maintaining, managing and controlling events that may degrade the security posture of the application.
- e) Training. Security training is provided on a continuous basis to keep users alert to the security requirements. Visual effects are used as constant reminders to ensure users always remain aware of their responsibilities.
- f) Physical Security. This consists of placing servers that contain privileged information in a secure and protected location, and to limit access to this location to individuals who have a need to access the servers. Since the server and data reside within a DON establishment, the strict security measures set by the establishment are always followed.

Servers are hosted at Defense Information Systems Agency Mechanicsburg, PA  
The current SSN Collection Justification Memo is valid.

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

Describe here.

## 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

Name:

Catherine M. Casper

Title:

Supervisory Program Manager

Organization:

NAVSEALOGCEN

Work Telephone Number:

717-605-7613

DSN:

430-7613

Email Address:

catherine.casper@navy.mil

Date of Review:

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

Name:

William Leidel

Title:

Activity Command Information Officer

Organization:

NAVSEALOGCEN

Work Telephone Number:

717-798-5946

DSN:

Email Address:

william.leidel@navy.mil

Date of Review:

CASPER.CATHERINE.M.1229112550  
Digitally signed by CASPER.CATHERINE.M.1229112550  
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN,  
cn=CASPER.CATHERINE.M.1229112550  
Date: 2015.01.26 09:19:16 -05'00'

LEIDEL.WILLIAM.E.1228703431  
Digitally signed by LEIDEL.WILLIAM.E.1228703431  
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,  
ou=USN, cn=LEIDEL.WILLIAM.E.1228703431  
Date: 2015.01.26 09:23:15 -05'00'

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

**ALEXANDER.DEXTER.C  
ARTER.1023648829**

Digitally signed by ALEXANDER.DEXTER.CARTER.1023648829  
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN,  
cn=ALEXANDER.DEXTER.CARTER.1023648829  
Date: 2016.02.23 10:43:09 -05'00'

Name:	Dexter Alexander
Title:	Deputy Director, NAVSEA Command Administrative Services
Organization:	SEA 00A
Work Telephone Number:	202-781-5200
DSN:	326-5200
Email Address:	dexter.alexander1@navy.mil
Date of Review:	23 Feb 2016

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

--

Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	

**Component Privacy Officer  
Signature**

**Robin Wade Patterson**

Digitally signed by Robin Wade Patterson  
DN: cn=Robin Wade Patterson, o, ou,  
email=patterson4010@comcast.net, c=US  
Date: 2016.03.07 17:58:11 -05'00'

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: 2016.03.09 14:58:59 -05'00'

Name:	for Lynda Pierce
Title:	Principal Deputy CIO
Organization:	Office of the Department of the Navy Chief Information Officer (DON CIO)
Work Telephone Number:	703-695-1892
DSN:	
Email Address:	lynda.pierce@navy.mil
Date of Review:	

**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](mailto: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.