



PRIVACY IMPACT ASSESSMENT (PIA)

For the

ENCHILADA DATABASE (ENCHILADA)

Department of the Navy - NAVSEA - NUWC DIVNPT

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

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
- 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

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

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:

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

Additional Authorities:

31 U.S.C. §3512, Executive agency accounting and other financial management reports and plans;
PL104-208 (Federal Financial Management Improvement Act (FFMIA) of 1996;
E.O. 10450, Security Requirements for Government Employees, in particular sections 2 - 9, and 14;
E.O. 12968, Access to Classified Information;
E.O. 13526, Classified National Security Information;
OMB Circular A-123; Management's Responsibility for Internal Control
HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors;
DoD 5200.2-R, Personnel Security Program Regulation;
DoD 5220.22-M, National Industrial Security Program (NISPOM);
DoDFMR 7000.14-R Vols 1 and 4;
SECNAVINST 5510.30B, Department of Navy Personnel Security Program;

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.

eNchilada provides a single point of access to Civilian Personnel information that is used throughout NUWC's business environment. The PII data is synchronized across NUWC's business organizations, eliminating redundant Civilian Personnel Data, placing access, creation, maintenance, retention, dissemination and disposal authority at the HRO Program Manager and/or User Representative level, and strictly controlling the access of PII. The PII is used to effect personnel transactions, establish employee rights and benefits governing Federal Civilian employment, process leave and overtime requests, ensure access to secure spaces is properly managed, manage Demonstration Project Incentive Pay and reconsiderations, and additional NUWC business and personnel management procedures.

From DITPR DON: Enchilada is composed of two applications, Enchilada and Security. Enchilada is a data repository providing secure access to information about NUWC employees and other persons of interest to NUWC and a mechanism for coordinating the activities of a broad spectrum of new and legacy information collection systems. The visible portion of Enchilada provides "one-stop shopping" for information and business applications from various source systems. Behind the scenes, Enchilada manages data security and the dissemination of information generated by one system to employees and other systems having an interest in the information. The Security application supports the Security Division's mission to implement access controls for a Level 1 Restricted Area in accordance with SECNAV M-5510.30, SECNAV M-5510.36, and OPNAVINST 5530.14D. It accomplishes this by providing a means for identifying authorized visitors, including those who are not in JPAS, to the guard force. It provides clearance information on employees to their supervisors, and a means of communicating changes in special access programs from program managers to the Security Division. It also manages information required to document the eligibility of DON military, civilian and certain affiliated employees for access to classified information and assignment to sensitive positions. It is the only information repository for military personnel assigned to the command. The primary contribution of Enchilada to NUWC is in its capabilities to provide up to the minute employee staffing information to all levels of enterprise management. Elements of the system are incorporated into the day-to-day activities of management decisions, including daily Request for Personnel Actions transactions distributed for processing to the Regional Human Resources Service Centers (HRSC) Fundamental to this contribution is the system's characteristic of providing the identical information about an employee in many different contexts. The various Human Resource (HR) applications includes: Action Suspense; Bring a Child To Work; Contractor Check-In Check-Out; DAWIA Demonstration Incentive Payout (DEMO-IP) & Reconsideration; Division On-Line Training – Human Resource Office (DOTS- HRO); Division On-Line Training (DOTS); Grievance Reporting Information Tracking System (GRITS); Level Descriptor Addendum (LDA); Mandatory On Line Training Medical Surveillance QRAM – Recruitment Report Tree SF50 Employee Distribution System.

The type of PII collected: Names, SSN (Full and Truncated), DoD ID number, citizenship, gender, race/ethnicity, birth date, place of birth, personal cell telephone number, home telephone number, personal email address, mailing/home address, security clearance, spouse and child information: name and age; disability information: type of disability; employment information: resume; emergency contact, education information: degree earned and proof of degree; Other: leave and overtime request and approval information, information required to determine access to secure spaces, information required to allow on-base attendance of DON dependent or sponsored children for Bring a Child to Work Day, etc.

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

The information collected is of no (government contact information) to high (SSN) risk to an individuals privacy. However, eNchilada is a MAC III Sensitive system and all required IA Controls for Confidentiality are in place. Examples include access control requires Program Manager and/or User Representative approval; PKI/CAC for authentication; The eNchilada Security Model tightly controls access to PII at the data attribute level.

Record creation, maintenance, retention, disposal, FOUO markings, controlled access, encryptions, prohibitions for use of non-government hardware / removal storage and PKI/CAC authentication are fully incorporated.

To safeguard this information the databases reside behind the NMCI ACL configured according to the C&A requirements on a server that is maintained in a secured, key-coded entry location. Access to the actual database requires a valid CAC, and associated local domain account. Accounts require a completed/approved SAAR-N form.

Users will be assigned roles which will only allow them to see the specific information that they require for their specific process, access to the actual PII data fields will be restricted by role.

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.

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.

Information directly requested from an employee by the application is covered by a Privacy Act Statement. The employee is notified that providing the information is voluntary.

Information collected from other sources was collected under Privacy Act Statements specific to those sources. The employee was notified of the voluntary nature of the collection at those sources.

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

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.

Information directly requested from an employee by the application is covered by a Privacy Act Statement. The employee was informed of the intended uses of that information collected at that time.

Information collected from other sources was collected under Privacy Act Statements specific to those sources. The employee was informed of the intended uses of that information collected at that time.

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

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

Privacy Act Statement **Privacy Advisory**
 Other **None**

Describe each applicable format.

The appropriate Privacy Act Statement is displayed with each associated module. For instance: The PAS for the Leave module is displayed on each page of the module. The PAS for Bring A Child To Work Day module is displayed on the form requesting the info.

PRIVACY ACT STATEMENT (for leave requests)

AUTHORITY: 10 U.S.C. §5013: Secretary of the Navy

PURPOSE: To collect information in order to initiate a leave request and approval action.

ROUTINE USES: In addition to the stated purpose, the information may be subject to those disclosures generally permitted under 5 U.S.C. §552a(b) of the Privacy Act. These records or information contained therein may be specifically disclosed outside the DoD as a routine use pursuant to 5 U.S.C. §552a(b)(3) as follows:

The DoD 'Blanket Routine Uses' that appear at the beginning of the Navy's compilation of systems of records notices apply to this system.

DISCLOSURE: Voluntary for all individuals. However, failure to provide the required information will result in not having a leave request submitted nor approved.

PRIVACY ACT STATEMENT (for Bring a Child to Work Day)
AUTHORITY: 10 U.S.C. §5013: Secretary of the Navy

PURPOSE: To collect information so that registrants may be admitted onboard and participate in the NUWC DIVNPT Bring A Child To Work events, and to ensure special needs are addressed where applicable.

ROUTINE USES: In addition to the stated purpose, the information may be subject to those disclosures generally permitted under 5 U.S.C. §552a(b) of the Privacy Act. These records or information contained therein may be specifically disclosed outside the DoD as a routine use pursuant to 5 U.S.C. §552a(b)(3) as follows:

The DoD 'Blanket Routine Uses' that appear at the beginning of the Navy's compilation of systems of records notices apply to this system.

DISCLOSURE: Voluntary for all individuals. However, failure to provide the required information will result in not being considered for participation in the NUWC DIVNPT Bring A Child To Work events. Failure to provide the requested special needs information may result in an inability to provide for special physical needs.

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.