



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

NAF_NEXCOM SYSTEM (NAF_NXS) Omni Channel E-commerce Application
--

Department of the Navy - NAVSUP - NEXCOM
--

### **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
- 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 N04066-5:

5 U.S.C. 301, Departmental Regulations  
10 U.S.C. 6011, Navy Regulations  
E.O. 9397 (SSN), as amended.

SORN N04066-6:

5 U.S.C. 301, Departmental Regulations  
29 U.S.C. 201  
29 U.S.C. 633a, Nondiscrimination on account of age in Federal Government Employment  
29 U.S.C. 791 Employment of individuals with disabilities  
29 U.S.C. 794a Remedies and attorney fees  
Pub.L. 93-259, Equal Employment Act of 1972  
E.O. 9397 (SSN), as amended.

**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 purpose of this DoD information system is to establish and utilize Navy Exchange E-commerce for online Order Management. Navy Exchange patrons utilize the site to purchase merchandise using the Internet and the E-commerce Call Center.

Personal information collected: Name, truncated SSN, other ID number (DoD ID Number is optional), gender, birth date, personal cell telephone number, home telephone number, personal email address, mailing/home address, credit card number.

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

The privacy risks associated with PII are limited to the Navy Exchange Omni-Channel system users entering data for customers. Minimizing the access and risks to PII data:

1. The user profiles must be created on the Navy Exchange Network system and the PII system.
2. The Oracle ATG platform systematically generate a user identification number when users are created.
3. Security groups are created and established according to the user's job position.
4. Credit card data is encrypted and tokenized in payment gateway.
5. Only the last four digits of the customer social security number is utilized during auth service call to NEXAUTH but not stored.
6. Patrons must be authenticated by the Navy Exchange NEXAUTH database.
7. System values are set: user profile expiration, system inactivity, password validation
8. Only system administrators have database accessibility.
9. Retina scans are generated and executed continuously in search of system and application vulnerabilities.
10. Order audits
11. Activity reports for Accounting and Customer Service.
12. NEXCOM second party file monitoring ReD (Retail Decisions) to prevent fraud
13. Fire wall settings and rules for users and hardware
14. Isolated Network
15. Payment Credit Industry (PCI) compliancy DDS

**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.

Speed Commerce. Standard NEXCOM contracting language. NEXCOM PII clauses are included in a contract as applicable when informed by the functional/technical experts that PII information will be involved.

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

Specify.

First Data Merchant Service (FDMS) - Major Credit Cards authorization and settlement  
Federal Express  
US Post Office

**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.

Customers have the right to not authenticate to mynavyexchange web store or uniforms site. Customers also must opt in to the mailing list in order for that data to be stored.

Without this information, the customer is unable to access the E-commerce web site or place an order at the call center.

(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.

Individuals have the opportunity to consent to the specific uses of their PII data if the customer is authorized via the Navy Exchange NEXAUTH database purchasing privileges are granted.

Customer consent is by nature of the mailing list application. If they opt-in, it directs NEXCOM to use the information supplied to send out digital flyer advertisements.

If the individual withholds their consent, the privilege to purchase merchandise via the Internet or the call

center is not permissible and they will not be able to receive flyers and other notifications.

(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.

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

Describe each applicable format.

A Privacy Act Statement (PAS) is provided to an individual when they are asked to provide PII. When a customer clicks sign in/register an account. As seen here <https://www.mynavyexchange.com/account/signin.jsp> the statement is toward the bottom of the page but above the footer.

**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.**