



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

|   |
|---|
| Infrastructure Business Operations Navy/NAVAIR/NAWC Support (IBONS) |
|---|

|  |
|--|
| Department of the Navy - NAVAIR - NAWCAD 7.2 |
|--|

### **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: NM05512-2 ; NM05512-1; NM08370-1; NM05000-2; N05230-1; DHRA-08; DMDC 10

NM05512-2, Badge and Access Control System Records (May 6, 2010, 75 FR 24932):

10 U.S.C. 5013, Secretary of the Navy  
10 U.S.C. 5041, Headquarters, Marine Corps  
OPNAVINST 5530.14C, Navy Physical Security  
Marine Corps Order P5530.14, Marine Corps Physical Security Program Manual  
E.O. 9397 (SSN), as amended

NM05512-1, Vehicle Parking Permit and License Control System (April 10, 2008, 73 FR 19482):

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

NM08370-1, Weapons Registration (February 19, 2008, 73 FR 9104):

10 U.S.C. 5013, Secretary of the Navy  
10 U.S.C. 5041, Headquarters, Marine Corps

E.O. 9397 (SSN), as amended

NM05000-2, Program Management and Locator System (January 24, 2008, 73 FR 419):

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

NN05230-1 Total Workforce Management Services (TWMS) (October 20, 2010, 75 FR 64715):

10 U.S.C. 5013, Secretary of the Navy  
10 U.S.C. 5041, Headquarters, Marine Corps  
CNICINST 5230.1, Total Workforce Management Services  
OPNAVINST 3440.17, Navy Installation Emergency Management Program  
E.O. 9397 (SSN), as amended.

DDHRA-08 Defense Travel System ( March 24, 2010, 75 FR 14142):

5 U.S.C. 5701-5757, Travel, Transportation, and Subsistence  
10 U.S.C. 135, Under Secretary of Defense (Comptroller)  
10 U.S.C. 136, Under Secretary of Defense (Personnel and Readiness)  
DoD Directive 5100.87, Department of Defense Human Resources Activity  
10 U.S.C. 3013, Secretary of the Army  
10 U.S.C. 5013, Secretary of the Navy  
10 U.S.C. 8013, Secretary of the Air Force  
DoD Financial Management Regulation 7000.14-R, Vol. 9, Travel Policies and Procedures  
DoD Directive 4500.09E, Transportation and Traffic Management  
DoD 4500.9-R, Defense Transportation Regulation, Parts I-V  
41 C.F.R. 300-304, Federal Travel Regulation  
Joint Federal Travel Regulation (Vol. 1) (Uniformed Service Members)  
Joint Travel Regulation (Vol. 2) (DoD Civilian Personnel)  
E.O. 9397 (SSN), as amended.

DMDC 10 DoD, Defense Biometric Identification System (DBIDS)( May 6, 2009, 74 FR 20930):

5 U.S.C. 301 Departmental regulations  
10 U.S.C. 113, Secretary of Defense, Note at Pub.L. 106-65  
10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness  
18 U.S.C. 1029, Fraud and related activity in connection with access devices  
18 U.S.C. 1030, Fraud and related activity in connection with computers  
40 U.S.C. Chapter 25, Information technology management  
50 U.S.C. Chapter 23, Internal Security  
Pub.L. 106-398, Government Information Security Act  
Pub.L. 100-235, Computer Security Act of 1987  
Pub. L. 99-474, Computer Fraud and Abuse Act  
E.O. 12958, Classified National Security Information as amended by E.O. 13142 and 13292  
E.O. 10450, Security Requirements for Government Employees  
E.O. 9397 (SSN), as amended

Other authorities:

NASPAXRIVINST 5510.15 - Regulations Governing Admission to Naval Air Station, Patuxent River, Webster Field, and Navy Recreation Center Solomons  
NASPAXRIVINST 5530.6 - Physical Security and Loss Prevention Standards  
NASPAXRIVINST 5560.2 - Administration of Traffic Regulations  
OPNAVINST 5530.14 - Navy Physical Security  
OPNAVINST 5560.10 - Standard Procedures for Registration and Marking of Non-Government Owned Motor Vehicles  
SECNAV 5510.30 - Department of the Navy (DON) Personnel Security Program (PSP) Regulation  
SECNAV 5510.34 - Manual for the Disclosure of Department of the Navy Military Information to Foreign

**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.

Due to Navy mandates to consolidate web sites, IBONS has multiple applications incorporated within it. One of the incorporated applications, BASICSII contains sensitive PII data. The responses in this document will only be related to the BASICSII application.

The servers supporting BASICSII and BASICS are located in the Information Technology / Information Management (IT/IM) Department at the Patuxent River Naval Air Station (NAS).

General descriptions of the applications covered by this PIA are:

BASICSII (Base Access Security Information Controls System II) – incorporated within IBONS - stores and supplies visitor and assigned personnel information for visitor control/base access purposes. BASICSII stores sensitive PII information and supplies it to the BASICS (Badging) client application described at the end of this section. BASICSII is used by the Pass Office to validate individuals requesting access to the base as well as to generate temporary passes, issue DOD vehicle decals and weapon permits. The application is used to record information on foreign national visitors to Patuxent River MD, Solomons MD, Webster Field MD. BASICSII supports Public Safety (Pass Office and Base Police); NAS Patuxent River Comptroller personnel responsible for granting Defense Travel System (DTS) accounts; NCIS and DOD investigators as well as Information Security (INFOSEC) and Operational Security (OPSEC) for personnel investigations including foreign nationals.

Personal information collected includes: name, other names used, SSN, driver's license number, other ID number, citizenship, legal status, gender, race/ethnicity, date of birth, place of birth, home telephone number, mailing/home address, and employment information.

Other personal information collected includes: foreign national data (visa number, passport number, invitational travel order number, naturalization number and date, alien registration number), vehicle information (vehicle identification number, license plate number, state and country), family member information, photograph and signature.

As a reference, the other applications incorporated within IBONS that do not store sensitive PII are:

IBONS – stores and supplies infrastructure/asset information for NAWC and NAVAIR buildings. IBONS stores business related PII (email address, phone number, title, employee type, org code) information for its account holders and for individuals designated as Point of Contacts for buildings in order to support automated processing of functional workflows. IBONS also stores business related PII (email address, phone number, title, rank/rate, pay plan/pay grade) for personnel assigned to NAWC/NAVAIR buildings for seat management purposes.

Range Sustainability – stores and supplies information regarding tracked aircraft and noise events, encroachment tracking, operational environmental planning and environmental review of planned events. Range Sustainability websites store business related PII (email address, org code and phone number) for their account holders.

MARS (Meeting and Resource Scheduler) – stores and supplies schedules, plans, space and personnel resources for meetings, events and conferences for the Protocol Office. MARS website stores business related PII (phone number) for their account holders and meeting attendees.

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

All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that IBONS/BASICSII, 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.

In order to safeguard privacy, access to the application data is provided on a need-to-know basis only. Accounts are granted application roles in order to further limit access to the data. All data is stored electronically. PII data is stored encrypted in the database. There are no paper documents used to store information. Additionally, DOD CAC cards are required for users to access the web site. All users have signed a System Authorization Access Request Navy (SAAR-N) or equivalent acknowledging their responsibility to safeguard information. All application screens reflecting PII data display the statement "Information contained herein is protected under the Privacy Act of 1974 and is For Official Use Only". Backup data is stored in secured facility. Failed hard drives are destroyed using prescribed security methods and the latest DON guidance. Servers supporting the application are on the NMCI network behind NMCI boundaries and are located in a secured facility. Server access is restricted to a small set of trusted administrators.

**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.

NAS Patuxent River Public Safety; Naval Criminal Investigative Services (NCIS); On-Site Contractors Automated Reporting (OSCAR) - DITPR # 1592

**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.

Individuals have the right to refuse to provide requested PII information. However, the individual may be refused access to the Base, which would be at the discretion of the Base Commander.

(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.

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

Information is only used for essential mission and administrative purposes

**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.

Provided to individual at time of request for base access.  
Base Access Security Information Control System (BASICSII) Privacy Act Statement  
AUTHORITY: 5 U.S.C. 301; E.O. 9397; 10 U.S.C. 113 Note at Pub.L. 106-65; 10 U.S.C. 136; 10 U.S.C. 5013; 10 U.S.C. 5041; 18 U.S.C. 1029; 18 U.S.C. 1030; 40 U.S.C. Chapter 25; 50 U.S.C. Chapter 23; Pub.L. 106-398; Pub.L. 100-235; Pub. L. 99-474; E.O. 12958 as amended by E.O. 13142 and 13292; E.O. 10450; Marine Corps Order P5530.14; NASPAXRIVINST 5510.15; NASPAXRIVINST 5530.6; NASPAXRIVINST 5560.2; OPNAVINST 5530.14; OPNAVINST 5560.10;

SECNAV 5510.30; SECNAV 5510.34

**PURPOSE:** The information contained herein will be used for providing individuals the privilege of installation access at Patuxent River Naval Air Station, to include Webster Field Annex and Navy Recreation Center Solomons.

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

To other federal, state, and local law enforcement agencies in the performance of official duties related to potential criminal investigations.

**MANDATORY OR VOLUNTARY DISCLOSURE AND EFFECT ON INDIVIDUAL NOT PROVIDING INFORMATION:** Disclosure of personal information is voluntary; however failure to provide information will result in denied access to the installation.

**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.**