



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Sierra Hotel Aircraft Readiness Program (SHARP)

Department of the Navy - COMPACFLT - CNAF (AIRLANT & AIRPAC)

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:

NM03760-1

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

NM03760-3

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
OPNAVINST 3710.7, NATOPS General Flight and Operating Instructions
E.O. 9397 (SSN), as amended.

Other authorities:

10 U.S.C 117, Readiness Reporting System: establishment Reporting to Congressional Committees
10 U.S.C. 113, Secretary of Defense
OPNAV Instruction 3501.360, Defense Readiness Reporting System - Navy (DRRS-N), dated

28 Jan 08.

CNAF Instruction 3500.1 Series, Squadron Training and Readiness

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.

Commander, Naval Air Forces, has directed the use of the SHARP V5.1 enterprise based squadron training/operations management system to support CNAF Instruction 3500.1 Series, Squadron Training and Readiness. This application's utility is to collect and maintain air crew log book information, identify execution of resources in support of training and readiness, and manage Fleet Readiness Squadron (FRS) based squadron training syllabi. At a minimum, SHARP V5.1 must collect, analyze and report squadron air crew readiness for consumption by DoD Directive 7730.65 for the Defense Readiness Reporting System (DRRS), Navy Training Information Management Systems (NTIMS), Status of Resources and Training System (SORTS), Naval Aviation Logistics Command Management Information System (NALCOMIS), and Naval Aviation Readiness Integrated Improvement Program (NAVRIIP).

SHARP collects the following personal information. Name, SSN (encrypted), Military Record Information (Call Sign, Rank, Rate, Unit, Crew Station/ACTC Level, Crew qualifications, Crew designations, flight data, Training and readiness data, TAD/leave).

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

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. Because of this possibility, appropriate security and access controls listed in this PIA are to be put in place. All systems are vulnerable to "insider threats." All System Managers will be vigilant to this threat by limiting system access to those individuals who have a defined need to access this information. There are defined criteria to identify who should have access to the applications. These individuals have gone through extensive background and employment checks.

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.

Naval and Marine Corps military, government and contractor personnel involved in naval aviation maintenance and the Navy Expeditionary Combat Command.

Other DoD Components.

Specify.

N/A

Other Federal Agencies.

Specify.

N/A

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 can object at the time they arrive at their squadron. Individuals could elect not to provide PII when applying for access; however, failure to provide the requested information may impede, delay, or prevent further processing of an account request and the tracking of their flight training.

(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.

Consent is provided once a pilot's PII is provided. PII is used when applying for account access and in the tracking of individual flight hours.

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 type="checkbox"/> None |

Describe each applicable format.

You are accessing a U.S. Government (USG) information system that is provided for USG-authorized use only.

By using this IS, you consent to the following conditions:

- The USG routinely monitors communications occurring on this IS, and any device attached to this IS, for purposes including, but not limited to, penetration testing, COMSEC monitoring, network defense, quality control, and employee misconduct, law enforcement, and counterintelligence investigations.
- At any time, the USG may inspect and/or seize data stored on this IS and any device attached to this IS.
- Communications occurring on or data stored on this IS, or any device attached to this IS, are not private. They are subject to routine monitoring and search.
- Any communications occurring on or data stored on this IS, or any device attached to this IS, may be disclosed or used for any USG-authorized purpose.
- Security protections may be utilized on this IS to protect certain interests that are important to the USG. For example, passwords, access cards, encryption or biometric access controls provide security for the benefit of the USG. These protections are not provided for your benefit or privacy and may be modified or eliminated at the USG's discretion. SHARP Software Requirements:
Browser: Internet Explorer 6.x
Cookies: Must be enabled
Scripting (Javascript): Must be enabled

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.

Note: the system only contains the requisite pieces of an individual's Military record, it DOES NOT contain the entire record.

Call Sign
 Rank
 Rate
 Unit
 Work email address
 Crew Station/ACTC Level
 Crew qualifications
 Crew designations
 Flight data
 Training and readiness data
 TAD / leave

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

The individual.

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

- | | |
|---|--|
| <input type="checkbox"/> Paper Form | <input checked="" type="checkbox"/> Face-to-Face Contact |
| <input type="checkbox"/> Telephone Interview | <input type="checkbox"/> Fax |
| <input type="checkbox"/> Email | <input checked="" 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)?

Data matching in order to capture an individual's flight information (training evolutions).

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

To capture mission related flight information related to an individual's training evolution.

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

If "Other," specify here.

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

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

If "Other," specify here.

(2) Technical Controls. Indicate all that apply.

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

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 type="checkbox"/> | Authorization to Operate (ATO) | Date Granted: | <div style="border: 1px solid black; height: 25px;"></div> |
| <input checked="" type="checkbox"/> | Interim Authorization to Operate (IATO) | Date Granted: | <div style="border: 1px solid black; padding: 2px;">Granted: 20131204
Expires: 20140604 +</div> |
| <input type="checkbox"/> | Denial of Authorization to Operate (DATO) | Date Granted: | <div style="border: 1px solid black; height: 25px;"></div> |
| <input type="checkbox"/> | Interim Authorization to Test (IATT) | Date Granted: | <div style="border: 1px solid black; height: 25px;"></div> |

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 - A pilot's personal information is entered by an SHARP administrator in order to set up an account for the individual.

Use - PII is used to control access to the application (manage system users) and associate aviation training data to a given aviation trainee.

Retention - All aviation records shall be maintain per SECNAV Manual 5210.1. The data is maintain by NAVAIRSYSCOM via the Naval Sea Logistics Centers Naval Flight Record Subsystem for an indefinite period.

Processing - SHARP does not process or aggregate any PII.

Disclosure - SHARP does not expose any PII data in the user interface.

Destruction - SHARP does not generate any media with PII that requires destruction. All electronic aviation records are maintained per SECNAV Records Management Manual 5210.1.

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

Access Controls: Access controls limit access to the application and/or specific functional areas of the all applications. These controls consist of privileges, general access, password 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. Access to information/records is limited to person (s) responsible for servicing analyzing the record in the performance of the official duties and who are properly screened and are cleared for the "need to know." Users are granted only those privileges that are necessary for their job requirements (e.g., need-to-know). The same roles that protect the database tables also determine what functionality is enabled for the users currently logged on.

Confidentiality: Confidentiality ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity: Integrity ensures that data has not been altered or destroyed in an unauthorized manner.

Audits: Audits to review and examine records, activities, and system parameters, to assess the adequacy of maintaining, managing, and controlling events that may degrade the security posture of the all applications.

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.

Physical Security: Physical security consists of placing servers that contain privileged information in a secure and protected location, to limit access to this location to individuals who would have a need to access the servers. Access to each application is limited to authorized and appropriately cleared personnel as determined by the system manager. Physical entry is restricted by use of locks, guards, and is accessible only to authorized, cleared personnel.

SHARP servers are located at the SPAWAR Data Center in San Diego, CA.

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

LEONARD.TIMOTHY.GIRO.11706631 08	Digitally signed by LEONARD.TIMOTHY.GIRO.1170663108 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=LEONARD.TIMOTHY.GIRO.1170663108 Date: 2014.05.22 09:49:18 -07'00'
-------------------------------------	--

Name:	Timothy G. Leonard
Title:	Training and Readiness Officer
Organization:	COMNAVAIRPAC N40D
Work Telephone Number:	619-767-7745
DSN:	577-7745
Email Address:	timothy.g.leonard@navy.mil
Date of Review:	22 May 2014

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)**

Digitally signed by FAN.TEREXA.LE.1242752100
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=FAN.TEREXA.LE.1242752100
Date: 2014.08.20 14:05:09 -07'00'

Name:

Terexa Fan

Title:

Staff Judge Advocate

Organization:

CNAFR/CNAP

Work Telephone Number:

619-545-2783

DSN:

Email Address:

terexa.fan@navy.mil

Date of Review:

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

MOULIS.NANCY.1172750164

Digitally signed by
MOULIS.NANCY.1172750164
DN: c=US, o=U.S. Government, ou=DoD,
ou=PKI, ou=USN,
cn=MOULIS.NANCY.1172750164
Date: 2014.08.20 13:41:06 -07'00'

Name:

Nancy Moulis

Title:

COMNAVAIRPAC IAM

Organization:

COMNAVAIRPAC N6

Work Telephone Number:

619-545-5034

DSN:

Email Address:

nancy.moulis@navy.mil

Date of Review:

**Component Privacy Officer
Signature**

**SHAW.MARY.P.122959734
1**

Digitally signed by SHAW.MARY.P.1229597341
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=USN, cn=SHAW.MARY.P.1229597341
Date: 2014.08.28 13:40:29 -04'00'

Name:

for Robin Patterson

Title:

Head, FOIA/Privacy Act Branch (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 Digitally signed by MUCK.STEVEN.ROBERT.1179488597
9488597 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=USN, cn=MUCK.STEVEN.ROBERT.1179488597
Date: 2014.09.10 12:54:00 -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.