



PRIVACY IMPACT ASSESSMENT (PIA)

For the

| |
|---|
| Flight Information Scheduling and Tracking (FIST) |
|---|

| |
|-----------------------------|
| U.S. Navy - NAVAIR - NAWCAD |
|-----------------------------|

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.

10 U.S.C. 5013, Secretary of the Navy

10 U.S.C. 5041, Headquarters, Marine Corps

OPNAVINST 3710.7U - NAVAL AIR TRAINING AND OPERATING PROCEDURES
STANDARDIZATION (NATOPS) GENERAL FLIGHT AND OPERATING INSTRUCTIONS

Executive Order 9397 - (SSN), as amended NUMBERING SYSTEM FOR FEDERAL ACCOUNTS
RELATING TO INDIVIDUAL PERSONS

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.

Naval Air Warfare Center, AD/WD, Flight Scheduling System. The objective of the Flight Information Scheduling and Tracking System (FIST) is to streamline the process of flight scheduling, record aircraft/air crew flight hours, and monitor air crew qualifications. FIST is essential to completing the aircraft test and evaluation mission for the Naval Air Warfare Center. Electronic collection of air crew SSN is required for the interface with Naval Aviation Logistics Command/Management Information System (NALCOMIS). FIST feeds NALCOMIS, it does not receive information from NALCOMIS. Collection of date of birth is required to accurately determine flight qualifications per the guidelines outlined in OPNAVINST 3710.7U. Flight data is used to compile a record of the individual's flight time, and to search and analyze for trends in order to improve aircraft maintenance, flight test analysis, and aviator readiness programs with the test squadrons under the authority of the Naval Air Warfare Center (NAWC).

(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.).

FIST stores the SSN of aircrew in order to feed air crew flight hours to NALCOMIS. The FIST application is available only within the NMCI enclave and access to it requires both a CAC and a user name and password to the system. The data is encrypted via https access. Quarterly account checks verify that all active accounts are still required users and remove access for any users that no longer require it. Additionally, the system uses roles to further restrict access to the PII to only those with a need to be able to access and update it.

Since FIST operates on the NMCI Network, 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. This risk is somewhat mitigated by setting up notification for the server team whenever the system is unavailable, so that they can verify that all security controls are put back in place after system restarts and patches.

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.

Data is sent to the NALCOMIS maintenance system within the test squadrons at NAVAIR. Data sent to NALCOMIS is done by event. Each event has aircrew data to tell who participated and in what role. That data is sent as SSN, last name and first initial of each crewmember. This is a one way interface, data is not retrieved from NALCOMIS.

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.

The following statement is on the access form:

"Authorization to allow collection of this information is voluntary."

Although, SSN is voluntary, flight data can not be collected without the PII data. OPNAVINST 3710.7U states, "Disclosure of this information is voluntary. However, failure to disclose this information can result in flight data not being recorded in the AV3M system and may result in loss of flight pay."

Once the access is granted the form is destroyed.

(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.

PII data contained in the system is provided for mission related use. The information is required to fulfill operational mission requirements.

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

Describe each applicable format.

OPNAV FORM 3760-31 is used to collect this information and contains the below paragraph:
Authority: The Department of Defense (DOD) is authorized to collect personal information under 5 U.S.C. 301 and Executive Order 10450 and 9397. **PRINCIPLE PURPOSES:** This information is being collected for the purpose of enabling DOD officials to make security determinations regarding your access to computer applications. **VOLUNTARY NATURE OF DISCLOSURE:** Authorization to allow collection of this information is voluntary. However, failure to allow collection of the required information may result in denial of access to computer applications. **DISCLOSURE OF SOCIAL SECURITY NUMBER:** Federal agencies are authorized by Executive Order 9397 to maintain systems of records to verify the identity of individuals. The furnishing of your social security number is voluntary on your part.

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.