



PRIVACY IMPACT ASSESSMENT (PIA)

For the

FLIGHT CLEARANCE PROCESSING SYSTEMS (FLIGHT CLEARANCE)

Department of the Navy - NAVAIR

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 authorities:

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

Other authorities:

OPNAV Instruction 3510.15 Series, Aviation-Series Naval Tactics, Techniques and Procedures Manuals and Naval Aviation Technical Information Product Program

OPNAV Instruction 3710.7 Series, NATOPS General Flight and Operating Instructions

NAVAIRINST 13034.1 Series, FLIGHT CLEARANCE POLICY FOR AIR VEHICLES AND AIRCRAFT SYSTEMS

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.

Any modification to a USN/USMC aircraft system, including increased capabilities, requires a Flight Clearance. This also includes urgent nonstandard repairs in theater. This DoD Information System (IS) automates the creation, editing, and routing of flight clearance requests from Fleet Type Commanders and Program Offices through the approval process. Once the clearance has been approved, all Interim Flight Clearance naval messages and NATOPS (Aircraft Flight Manuals) Revisions are automatically posted to the flight clearance application (web site) for fleet and NAVAIR users to download and review their clearance to use a new system on their aircraft as well as learn Safety of Flight information. NATOPS Interim Change messages and Naval Aviation Technical Information Product (NATIP) (Weapon/Mission System Manuals) released announcements are manually posted to the flight clearance application immediately after they are approved for the same purpose as NATOPS Revisions and Interim Flight Clearances automatic posting. The information collected (checked in Section 3.a of this Form) is required for accountability and in order for users to be contacted in order to carry out the missions applicable to the Instructions listed in section 2.f.(2) (c). Personal Phone numbers and e-mail address are often required to notify personnel of pending actions to satisfy after hours, weekend, and holiday requests. Air-4.0P is a 24/7 operation whose office and support personnel must have access to Flight Clearance stakeholders when needed. AIR-4.0P is accountable in NAVAIR's AIR-4.0 COOP to execute this process under any circumstances and conditions which also requires the staff to access emergency contact information remotely.

This system is currently limited to US citizens only. It is a requirement for requestors to provide country of citizenship before being granted access due to the requirement to comply with Distribution Statement markings on the documents available on this site. Although it is not explicitly stated for each user in the Points of Contact listings that each individual is a US citizen, it can be inferred due to the requirement stated above.

Personal information collected includes: Name, citizenship, personal cell telephone number, home telephone number, personal e-mail address, and employment information.

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

The risk to privacy is a user piecing together information using information from this system as a starting point. General users only have access to contact information listed as work and/or primary information. This means general users only know citizenship and work phone/e-mail unless personnel registering for access to the site opt to list their cell phone or home phone as their primary number.

All users, regardless of their empowerment within the site must go through BigIP/PKI.

AIR-4.0P staff may also be empowered to access and maintain the PII listed in Section 3.a. This permission is granted to users who may have the need to process a Flight Clearance during nonworking hours. Only staff approved by AIR-4.0P may access this data. A smaller number of Department Staff may change this data in addition to the individuals users who are updating their own profiles.

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.

This information is available to any DON user from any NAVAIR Command and any rank (Mil and Civ) who have been individually approved by AIR-4.0P to retrieve personal contact information.

Other DoD Components.

Specify.

This information is available to any DoD user from any Command and any rank if they have a need to know with respect to the technical information on the Information System (Mil and Civ) who have been individually approved by AIR-4.0P to retrieve personal contact information.

Other Federal Agencies.

Specify.

Federal Agencies that own and operate aircraft systems that NAVAIR procured or support for testing may access this Information System. This includes, but is not limited to U.S. Department of Homeland Security - U.S. Coast Guard, NASA, Department of Energy who have been individually approved by AIR-4.0P to retrieve personal contact information.

State and Local Agencies.

Specify.

Contractor (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Any contractors supporting DoD components or other federal agencies with an official need to know may access this data once approved on an individual basis. All contractors must obtain a signature from their Contracting Office Representative before being granted access as a general user and AIR-4.0P approves them individually for any additional privileges. Contract M clauses address safeguarding PII, training requirements, etc.

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.

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

PII is required in order to support 24/7 flight clearance process.

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 is required in order to support 24/7 flight clearance process.

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.

Pop-up when entering site is the following "DoD Warning Banner".
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
At any time, the USG may inspect and seize data stored on this IS.
Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants.

Conditions, Restrictions, and Disclaimers
Areas of this Server link to other Web Information Systems providing security-related information operated by other government organizations, commercial firms, educational institutions, and private parties. We have no control over the information on those systems which may be objectionable or which may not otherwise conform to Department of Navy policies. Unless otherwise noted, some of

the Sites listed within the pages of this server are provided by organizations outside the Navy Domain. These links are offered as a convenience and for informational purposes only. Their inclusion here does not constitute an endorsement or an approval by the Department of the Navy of any of the products, services, or opinions of the external providers. The Department of the Navy bears no responsibility for the accuracy or the content of external sites.

Privacy & Security Notice

This is a U.S. Department of Defense computer system. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. Government uses. DoD computer systems may be monitored for all lawful purposes, including ensuring that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

Privacy Policy

This is a World Wide Website for official information about the NATIP, NATOPS, and the IFC Program Offices. It is provided as a public service by the Airworthiness Program Office. The purpose is to provide information and news about Airworthiness to authorized users.

This system, and the data contained herein, will be used for official use and authorized purposes in accordance with the Joint Ethics Regulation, paragraph 2-301, Use of Federal Government Resources. Conveyance of any information contained in this system is authorized to U.S. Government Agencies and their contractors to protect technical or operational data or information from automatic dissemination under The International Exchange Program, or by other means, as determined by the Commander, Naval Air Systems Command. Other requests for these documents, including all requests for foreign disclosure, shall be referred to the Airworthiness Officer, Airworthiness Office, AIR 4.0P, Bldg 460, Naval Air Systems Command, 22244 Cedar Point Road, Patuxent River, MD 20670-1906.

Unauthorized attempts to upload information or change information on this Website are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.

For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

Except for authorized law enforcement investigation and to maintain required correspondence files, no other attempts are made to identify individual users or their usage habits. Raw data logs are used to simply determine how many users are accessing the site, which pages are the most popular, and, from time to time, from which top level domain users are coming. This data is scheduled for regular destruction in accordance with National Archives and Records Administration guidelines.

Privacy Act Statement (PAS)

Authority: 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; OPNAV Instruction 3510.15 Series, Aviation-Series Naval Tactics, Techniques and Procedures Manuals and Naval Aviation Technical Information Product Program; OPNAV Instruction 3710.7 Series, NATOPS General Flight and Operating Instructions; NAVAIRINST 13034.1 Series, FLIGHT CLEARANCE POLICY FOR AIR VEHICLES AND AIRCRAFT SYSTEMS; and SORN N05230-1.

Purpose: Command management and support of flight clearances and operations, personnel qualifications and assignments.

Routine Uses: Information will be accessible to command management and staff with a need to know to manage and support command flight clearance operations and assignments.

Disclosure: Voluntary; however, failure to provide the required requested information will result in the inability to receive an Airworthiness account.

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.