PRIVACY IMPACT ASSESSMENT (PIA)

For the

Joint Primary Aircraft Training System - Training Integrated Management System (JPATS-TIMS)
Department of the Navy - COMPACFLT - CNATRA N6, N7

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	DITPR ID: 1568 DITPR DON ID: 19385
□ **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 UII: 007-000003497

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 N01542-1

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 N01542-1 authorities:

5 U.S.C. 301 Departmental Regulations
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 JPATS-TIMS is to maintain a listing of training, education and qualifications of military service members who either provide or receive Naval Aviation Training. The personal information is intended for use by Naval Aviation program managers and authorized users of the system. This system will also be used to provide projections of training resources. It captures, collates, and supports the evaluation of training and records student and instructor Naval Aviation accomplishments for trainees/trainers.

The System Executive Agency is the USAF, while CNATRA has a separate deployment of JPATS-TIMS at its Headquarters and each of its five Training Air Wings (TRAWING). The departmental databases located at each TRAWING replicates data to the CNATRA Headquarters data repository.

JPATS-TIMS as implemented at CNATRA resides on the NETC- TRANET(U)_infrastructure, as well as the DON NMCI infrastructure.

Interfaces include CeTARS, NALCOMIS, AV3M, NITRAS, and applications under the CNATRA HQ-DSS system. PII collected by JPATS-TIMS comes directly from HQ-DSS.

Components are located at CNATRA HQ in NAS Corpus Christi, TX, five TRAWING sites located at NAS Corpus Christi TX, NAS Pensacola, FL, NAS Whiting Field, Milton, FL, NAS Kingsville TX, and NAS Meridian, MS.

PII collected includes the following: Name, other names used, SSN (truncated), DoD ID Number (EDIPI), Officer File Number, citizenship, legal status, gender, race/ethnicity, birth date, place of birth, personal cell telephone number, home telephone number, personal e-mail address, mailing/home address, religious preference, security clearance, spouse information: name; marital status, child information: number of dependents and names; medical and disability information: Waivers-The medical conditions that have been approved for a pilot to continue flying; military records: Grade, Date of Rank, Military Designation Code, Military Designation Date, Home Base; education information: name of school and/or university and emergency contact: Point of Contact, POC Phone Number.

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

The principal threat to JPATS-TIMS is adjudged to be the insider threat. Disgruntled personnel pose another threat, especially those who are terminated for cause. The most common threat is that posed by users of the system who negligently or inadvertently fail to follow security requirements for the handling and labeling of system output or media, or the rules against the introduction of unauthorized software or data. There is the threat arising from the failure of authorized users to employ proper procedures for the entry or manipulation of system data arising due to failure of users to be properly trained in the use and operation of the system.

Various security measures have been implemented to ensure PII/PA data processed by the system is properly safeguarded. Access to the JPATS-TIMS system is granted only to those users with a need-to-know. Users are granted access based on job requirements utilizing the concept of least privilege. Security awareness training is provided on a continuous basis to inform and remind users of security requirements for safeguarding and protecting PII/PA data. The JPATS-TIMS systems housing PII/PA data are located within secure environments. Access is limited to authorized users with a need-to-know.

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. Training records are shared within the Naval Aviation Training Command by designated Program Managers and Naval Aviation personnel.

☒ **Other DoD Components.**

Specify. Student records will be shared between DOD components, to include USN, USAF, USCG and USMC based on student aviators and instructor pilots that are enrolled in the Naval Aviation training program under CNATRA.

☒ **Other Federal Agencies.**

Specify. Federal Records Center

☐ **State and Local Agencies.**

Specify.

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

Specify. Northrop Grumman is the contractor charged with support and maintenance of the TIMS application. However, they are subject to a Non-disclosure agreement.

☐ **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 not collected directly from the individual. PII is pulled electronically from another system (CETARS) and the TIMS Functional Administrator or Wing Student Control (STUCON) can update an individual's PII.

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 not collected directly from the individual. PII is pulled electronically from another system (CETARS) and the TIMS Functional Administrator or Wing Student Control (STUCON) can update an individual's PII.

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.

PII is not collected directly from the individual. PII is pulled electronically from another system (CETARS) and the TIMS Functional Administrator or Wing Student Control (STUCON) can update an individual's PII.

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.