PRIVACY IMPACT ASSESSMENT (PIA)

For the

Student Qualification Requirement Information Performance Tracking (SQRIPT)
Department of the Navy - TMA DHP Funded System - BUMED

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 | DADMS ID #: 47698 |

☐   **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 <u>retrieved</u> by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒   **Yes**   ☐   **No**

If "Yes," enter Privacy Act SORN Identifier | NM01500-2 and NM05100-4 |

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:

NM01500-2:

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps function, composition
OPNAVINST 1510.10B, Corporate Enterprise Training Activity Resource System (CeTARS), Catalog of Navy Training Courses and Student Reporting Requirements
MCO 1580.7D Schools Inter-service Training
E.O. 9397 (SSN), as amended

NM05100-4:

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
E.O. 9397 (SSN)
E.O. 12196, Occupational Safety and Health Programs for Federal Employees
DoD Instruction 6055.7, Accident Investigation, Reporting, and Record Keeping
OPNAVINST 5102.1 series, Mishap Investigation and Reporting
MCO P5102.1B, Marine Corps Ground Mishap Investigation and Reporting Manual.

Other Authorities:

OPNAVINST 3710.7, Naval Air Training and Operating Procedures Standardization (NATOPS) Manual, Chapter 8, Aeromedical and Survival

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.

SQRIPT (Student Qualification Requirement Information Performance Tracking System) is a GOTS (Government Off-the-Shelf) web application with underlying database structures that records and houses short-term training data input across the eight ASTC (Aviation Survival Training Center) sites. SQRIPT provides an interface to ASTCs in order to meet their requirements of training management. SQRIPT tracks the NSTI (Naval Aviation Survival Training Institute) program, which includes mishap data, high-risk training for NSTI Instructors (Dunker, LPC (Low Pressure Chamber), etc), student qualifications, and air crew data as dictated by OPNAVINST 3710.7. The need to record, track and report on BUMED SOP (Bureau of Medicine Standard Operating Procedure) data was started at the beginning of derived training curriculums. SQRIPT will pull data from and push data to Corporate Enterprise Training Activity Resource System (CeTARs).

The types of PII collected in the system include name, address, marital status, birth date, social security number, gender, medical and mishap information and military records which include status of student qualifications and class.

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

SQRIPT is at risk because all systems may be vulnerable to unauthorized intrusion and hacking. There are risks that SQRIPT, with its collection of PII, could be compromised. Because of this possibility, appropriate security and access controls listed in this PIA have been put in place such as the use of DoD CAC certificates, secure data transmission and national DoD security standards.

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. | CeTARS (Corporate Enterprise Training Activity Resource System) which is an existing DON NETC information system.

☐ **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.
| LOCKHEED MARTIN CONTRACT FY11 |
| SECTION H SPECIAL CONTRACT REQUIREMENTS |
| Privacy Act Compliance paragraphs as follows: |
| The contractor shall ensure that employees assigned to this task understand |
| and comply with DOD Regulation 5400.7, DOD Freedom of Information Act |
| Program and SECNAVINST 5211.5E, Department of the Navy (DON) Privacy |
| Program. These directives set policy and procedures for the disclosure of |
| records to the public and for making, handling, transmitting, and |
| safeguarding For Official Use Only (FOUO) material. In addition, they set |
| guidelines for collecting, safeguarding, maintaining, using, accessing, |
| amending, and disseminating personal data kept in systems of records. |

☐ **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.

| Personal information is not collected directly from the individual. |

(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.

```
Personal information is not collected directly from the individual.
```

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.

```
Personal information is not collected directly from the individual..
```

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.